Universidad Carlos III de Madrid
www.uc3m.es

TRABAJO DE FIN DE GRADO

AUTENTICACIÓN BIOMÉTRICA PARA COMUNICACIONES INALÁMBRICAS A TRAVÉS DE NFC

GRADO EN INGENIERÍA TELEMÁTICA

Autor: Daniel Sierra Ramos

Tutor: Raúl Sánchez Reíllo

Leganés, 10 de Junio de 2012

Título: Autenticación biométrica para comunicaciones inalámbricas a través de NFC

Autor: Daniel Sierra Ramos

Tutor: Raúl Sánchez Reíllo

EL TRIBUNAL

Presidente:

Vocal:

Secretario:

Realizado el acto de defensa y lectura del Trabajo Fin de Grado el día __ de Julio de 2013 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

A mis padres, Gabriel y Lucía

A mi hermana Irene

A mi novia Sara

A mis amigos y gutitos

Por vuestro apoyo incondicional

La verdadera sabiduría está en reconocer la propia ignorancia

- Aristóteles -

RESUMEN

Este Trabajo de Fin de Grado tiene como objetivo realizar el desarrollo de un sistema de transacciones a modo de monedero electrónico mediante el uso de la tecnología NFC en teléfonos móviles. El sistema hace uso de la tarjeta SIM NFC del dispositivo para almacenar la información referente al monedero y para realizar todas las operaciones de crédito y débito de forma segura en nuestro propio teléfono. Para una mayor seguridad, el sistema incorpora un mecanismo de autenticación biométrica conforme a la filosofía "Match-on-card" la cual permite al usuario autenticarse biométricamente. En nuestro caso, esta autenticación biométrica se realizará con reconocimiento de Iris, realizando la comparación en la tarjeta SIM del propio dispositivo del usuario, evitando así sacar información sensible al exterior.

El sistema consta de dos dispositivos móviles, uno actuando como punto de venta, y otro como cliente. En punto de venta, al que llamaremos sistema servidor, simula una máquina expendedora de bebidas, mientras que el cliente hace uso de un dispositivo móvil con la tarjeta SIM NFC que permite interaccionar con el servidor de forma inalámbrica. Asimismo el dispositivo cliente lleva implementado un software de gestión que habilita al usuario para realizar consultas del estado de su monedero electrónico así como para autenticarse biométricamente mediante Iris.

ABSTRACT

This Final Degree Project aims to develop a trading system by using NFC technologies on mobile phones. The system works with the device SIM card in order to store the state of the electronic wallet and to perform all credit and debit operations securely inside our own phone. Moreover, the system incorporates a biometric authentication mechanism according to the "Match-on-card" philosophy which allows the user to authenticate himself biometrically by using an iris recognition algorithm.

The system has two mobile devices, one of them acting like a point of sale and the other like a client. The point of sale (server) simulates the software of a soft-drink vending machine. The client consist of two main elements: a mobile device and a SIM NFC card, which allow to communicate with the server wirelessly. Additionally the client device implements a management software that allow the user to make enquiries and perform biometrical authentications and enrolments.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTADO DE ACRÓNIMOS

ADN	Ácido Desoxirribonucleico
APDU	Application Protocol Data Unit
API	Application Programming Interface
C – APDU	Command APDU
CAD	Card Acceptance Device
CLF	Contactless Frontend
CP8	Computadora Portátil de los 80
DoS	Denial of Service
ECMA	European Computer Manufacturers Association
EEPROM	Electrically-Erasable Programmable Read Only Memory
EPROM	Erasable Programmable Read Only Memory
ETSI	European Telecommunication Standards Institute
GP	GlobalPlatform
GSM	Global System for Mobile Communications
HCI	Host Controller Interface
IEC	International Electrothecnical Consortium
ISD	Issuer Security Domain
ISM	Industrial, Scientific and Medical (radio band)
ISO	International Organization for Standardization
JIS	Japanese Industrial Standards
LLCP	Logical Link Control Protocol
NDEF	NFC Data Exchange Format

NFC	Near Field Communication
OHA	Open Handset Alliance
PIN	Personal Identification Number
POS	Point Of Sale
R – APDU	Response APDU
RAM	Random Access Memory
RFID	Radio Frequency Identifier
ROM	Read Only Memory
RTD	Record Type Definition
SEEK	Secure Element Evaluation Kit
SIM	Subscriber Identity Module
SOTI	Sistema Operativo de Tarjeta Inteligente
SWP	Single Wire Protocol
TI	Tarjeta Inteligente
UICC	Universal Integrated Circuit Card
Wi-Fi	Wireless Fidelity
XML	eXtensible Markup Language

1. INTRODUCCIÓN

Existen muchas maneras de identificar un usuario, desde las clásicas tarjetas de visita hasta los complejos y sofisticados mecanismos biométricos de autenticación, incluyendo las tarjetas inteligentes y otras soluciones seguras. Las tecnologías de identificación están muy extendidas en nuestra sociedad. Podemos encontrarlas en numerosos escenarios tales como cuando realizamos una operación bancaria o cuando accedemos a una sala securizada en nuestro lugar de trabajo. Estas tecnologías proporcionan una importante medida de proteger nuestra información personal y de restringir el acceso a lugares confidenciales.

Hoy día casi todo el mundo posee una tarjeta inteligente. Estos trozos de plástico se han convertido en una importante parte de nosotros en nuestras tareas diarias. Con estas tarjetas podemos realizar numerosas operaciones tales como pagos, acumular puntos de nuestra gasolinera favorita, identificarnos a través del carnet de identidad o realizar una llamada a través de nuestra tarjeta SIM. Además, todas estas operaciones podemos realizarlas de manera segura gracias a los numerosos mecanismos de seguridad incluidos en las tarjetas tales como números PIN o firmas digitales.

Como se menciona anteriormente, la gran mayoría de tarjetas inteligentes poseen un número PIN como medida de seguridad pero, ¿es el número PIN realmente seguro? ¿Existe algún otro mecanismo de autenticación más seguro? La respuesta es sí: con la biometría es posible.

La biometría es una tecnología relativamente joven y emergente que emplea uno o varios rasgos de las personas para realizar las tareas de reconocimiento en un sistema. Existen numerosas modalidades biométricas como iris, huella dactilar, geometría de la mano, reconocimiento facial o incluso comparación de ADN. Cada una de las diferentes modalidades tiene sus propias características y resulta adecuado para diferentes tipos de sistemas y requisitos. La identificación biométrica permite obtener un extra de seguridad en un sistema, pero ¿dónde podemos emplear esta tecnología? ¿Podemos combinar tarjetas inteligentes y biometría? La respuesta está en los sistemas “Match-on-card”, los

cuales nos permiten incluir mecanismos de autenticación biométrica en tarjetas inteligentes.

El estándar NFC (Near Field Communication) describe la comunicación a corta distancia entre dispositivos móviles y tarjetas inteligentes inalámbricas. Esta tecnología está siendo implementada en los últimos smartphones añadiendo la posibilidad de comunicación con otros dispositivos. NFC está siendo ampliamente aceptado por los usuarios ya que constituye una poderosa herramienta para realizar transacciones de forma segura e inalámbrica, especialmente en combinación con las tarjetas inteligentes y la biometría.

En este documento se muestra el desarrollo de la implementación de un sistema de pagos basado en tecnologías inalámbricas y de identificación tales como NFC y biometría. Primeramente se hace una pequeña introducción al estado actual de diversas tecnologías como NFC, el sistema operativo Android, las tarjetas inteligentes y los sistemas biométricos. A continuación, en el seno del documento, se explicará la implementación de un sistema real de transacciones empleando la tecnología NFC y los sistemas “Match-on-card”. Finalmente, una breve concusión hará alusión a la situación del proyecto y a la perspectiva de su implementación en un contexto real.

2. INTRODUCTION

There are many ways to identify a user, from the classic business cards to the sophisticated biometric mechanisms of authentication, including smartcards or other solutions with better security features that business cards. Identification technologies are quite extended in our society. We can find them in several scenarios, such as when performing a payment operation or when entering into a secured laboratory in our workplace. These technologies provide an important countermeasure to protect our personal or confidential information or to restrict the access to high secured facilities

Nowadays almost everybody have a smartcard. These plastic cards have become an important part of us in our daily life. With these cards we can perform many operations like payments, accumulating points of our favourite gas station, identifying ourselves through the passport or ID card or performing calls through our SIM card. Moreover, to guarantee security, some smartcards include a security mechanism based on a personal number used to grant the user access to the system (the PIN: Personal Identification Number).

As mentioned above, smartcards have a personal identification number to grant the access to the genuine user but, is this PIN security really secure? Can we use another and more secured mechanism of authentication? The answer is yes: biometrics can offer that possibility.

Biometrics is a relatively young and emerging technology that uses one or several person traits to perform the recognition task in a system. There are many biometric modalities like iris, fingerprint, hand geometry, face recognition or even DNA matching. Each of the different modalities has its features and can be suitable for different systems and requisites. Biometric identification grants a security plus in a system, but where can we use this technology? Can we combine smartcards and biometrics? The answer again is positive and can be found in match-on-card systems. Match-on-cards systems include the biometric authentication mechanisms in a smartcard. This allow us to

NFC stands for Near Field Communication. NFC is a standard that describe the wireless short range communication among mobile devices and wireless smartcards. This technology is being implemented in the latest smartphones to add the ability of communicate with another devices or smartcards. NFC is being accepted by the users and involves a powerful tool to perform secured transactions wirelessly especially in addition to biometrics and smartcards.

In this document we will show the work developed for implementing a payment system based on wireless and identification technologies like NFC and biometrics. Firstly, the state-of-art of smartcards, NFC and Android operating system is explained. Then, the main content of this document will be explained. In this section, we will go through the implementation of a real system of payments using NFC and a match-on-card solution. Finally we will finish with a brief conclusion of the situation of this project and the perspective for its implementation in a real context.

3. ESTADO DEL ARTE

3.1 Tarjetas inteligentes

Una tarjeta inteligente es un dispositivo, generalmente de plástico, capaz de almacenar y procesar información digital de forma segura. Actualmente estos dispositivos están a la orden del día y constituyen una forma cómoda y rápida de realizar las operaciones más habituales de nuestro día a día. Un ejemplo de ello son las archiconocidas tarjetas bancarias, con las que podemos realizar todo tipo de transacciones y pagos, o la propia tarjeta SIM de nuestro teléfono móvil, la cual nos permite comunicarnos de forma inalámbrica con cualquier persona en cualquier lugar del mundo gracias a nuestro teléfono móvil.

3.1.1 Orígenes y evolución

Las tarjetas inteligentes son un tipo de tarjetas con circuito integrado, al igual que las tarjetas de memoria, con la salvedad de que estas últimas no contienen un microprocesador, y por tanto, no tienen la capacidad de procesar información.

Las tarjetas inteligentes surgen entre los años 1976 y 1978 de la mano del fabricante CII Honeywell Bull en conjunto con un ingeniero llamado Eugene Michel y la empresa Motorola. La primera tarjeta contaba con un microprocesador con arquitectura 6805 y una memoria de 1KB. Por otro lado, el fabricante comienza también a trabajar con este tipo de tarjetas con microprocesador creando sus propias tarjetas basadas en la arquitectura 8021 de Intel, posteriormente sustituida por la 8051, y una memoria de 2KB.

Durante los años siguientes los fabricantes intentaron mejorar sus prototipos de tarjeta e intentar reducir su tamaño. No fue hasta principios de los 80 cuando Bull consiguió presentar una tarjeta de las mismas dimensiones que las de banda magnética conocida como CP8 (*Computadora Portátil de los 80*) la cual tuvo gran aceptación y, dado que por aquel entonces empezó a avanzar la tecnología microelectrónica, aumentó el desarrollo de chips y su adaptación a las normas ISO, lao permitió hacer aptas las tarjetas para ser empleadas en los mismos cajeros que las de banda magnética.

3.1.2 Características

Las tarjetas inteligentes constan de un circuito integrado formado por un microcontrolador, es decir, un microprocesador y una serie de periféricos asociados tales como memorias, bloques de entrada y salida, sistemas de control de alimentación, etc. Y, en algunos casos, hay tarjetas que cuentan con un módulo de procesamiento adicional encargado de realizar operaciones criptográficas de alto coste computacional (*véase Figura 1: Bloques de una TI*).

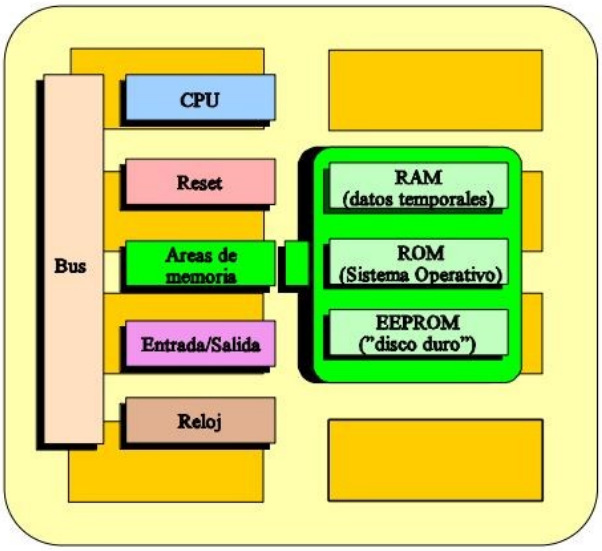

Figura 1: Bloques de una TI [1]

Una parte importante de las tarjetas, aparte del microprocesador, son las memorias de almacenamiento. Actualmente, las tarjetas inteligentes cuentan con una memoria de almacenamiento EEPROM en la que se puede almacenar información persistente que puede ser sobrescrita por el usuario en cualquier momento de la vida de la tarjeta, haciéndola así reutilizable. Asimismo, las tarjetas cuentan con una memoria ROM, en la cual se encuentra almacenado el SOTI (*Sistema Operativo de la Tarjeta Inteligente*). Existen diferentes tipos de SOTI, cada uno empleado en un área determinada, pero el que más nos interesa a nosotros dentro del alcance de este TFG es el sistema JavaCard, del cual se hablará más adelante. Asimismo, y no menos importante, podemos encontrar la memoria RAM de la tarjeta, la cual es empleada por el microprocesador para almacenar la información referente a los procesos y aplicaciones en ejecución del sistema, así como el buffer de comunicaciones.

3.1.3 Tipos de tarjetas

Las tarjetas inteligentes se pueden clasificar en varios grupos. Los más importantes son los siguientes:

a) Según su interfaz

- *Tarjetas con contactos:* Son las más antiguas y su interfaz de comunicación consta de una serie de pines metálicos que sirven para transmitir y recibir datos de un CAD (*Card Aceptance Device*), también conocido como lector. Estas tarjetas se comunican de acuerdo a la extendida norma internacional ISO/IEC 7816 por la que se establecen las dimensiones, especificaciones, mecanismos de comunicación, etc. de una tarjeta inteligente. Para este TFG se emplearán este tipo de tarjetas con una importante particularidad, que es la capacidad de establecer una comunicación con el chip NFC de un dispositivo móvil mediante uno de los pines.

- *Tarjetas sin contactos:* Estas tarjetas presentan una interfaz inalámbrica como medio de comunicación. El modelo más extendido se rige por la norma ISO/IEC 14443.
- *Tarjetas híbridas:* Son las tarjetas más actuales ya que disponen de las dos interfaces de comunicación arriba mencionadas. Funcionan tanto de forma inalámbrica como introduciéndolas en la ranura de un CAD.

b) Según su tamaño

Según la norma ISO/IEC 7816-1 existen tres tipos de tamaño en una TI:

- *ID 000:* Es el tamaño de las tarjetas SIM empleadas en GSM. También se conoce como formato plug-in.
- *ID 00:* Es un tamaño medio muy poco extendido
- *ID 1:* Es el tamaño más común empleado en las tarjetas bancarias

En este TFG son de especial interés las tarjetas SIM NFC, es decir, unas tarjetas de la norma ID000 que presentan la capacidad de comunicarse con el chip NFC de un dispositivo móvil mediante uno de sus pines metálicos. Este tipo de tarjetas se explicarán en detalle en posteriores apartados.

3.1.4 JavaCard

JavaCard es una tecnología que nos permite ejecutar pequeñas aplicaciones Java llamadas "applets" en una tarjeta inteligente de forma segura. Estos "applets" se pueden emplear para diversas aplicaciones de la vida real como la realización de pagos o la identificación de personas en un sistema.

JavaCard proporciona una forma relativamente sencilla de programar aplicaciones dentro de las tarjetas (es decir, ampliando las funcionalidades del su sistema operativo) ya que nos brinda las ventajas del lenguaje Java. Por otro lado, hay que tener en cuenta que JavaCard nos proporciona solamente algunas funcionalidades básicas de Java, debido a la escasez de recursos en una tarjeta inteligente.

Además de esto, JavaCard nos ofrece una forma segura de ejecutar "applets" en la tarjeta ya que proporciona lo que se denominan contextos de aplicaciones. Un contexto puede contener una o varias aplicaciones, y la particularidad que tiene es que una aplicación no puede acceder a los datos almacenados en otra aplicación de un contexto diferente, a no ser que se empleen mecanismos habilitados para ello (interfaces compartidas). De esta manera se proporciona un mecanismo de aislamiento aumentando así la seguridad.

La comunicación de un "applet" con el exterior (por ejemplo un PC) se realiza mediante comandos, empleando la estructura de intercambio de APDUs definida en la norma ISO/IEC 7816-4. Este protocolo define dos tipos de unidades de datos, los C-APDU y los R-APDU. Los primeros son los comandos que se envían desde el exterior a la tarjeta, y los segundos son las respuestas que la tarjeta devuelve a dichos comandos. Basándose en este protocolo, se define una gran variedad de comandos y respuestas en diversos estándares, tales como las distintas partes de la ISO/IEC 7816 o GlobalPlatform pero, además, en el caso de JavaCard, somos nosotros los que podemos definir nuestros propios comandos y respuestas, siempre que se cumplan las reglas generales especificadas en ISO/IEC 7816-4.

El formato de los comandos y respuestas están definidos en la ISO/IEC 7816 (*véase "Figura 2: Comando APDU y Respuesta APDU"*).

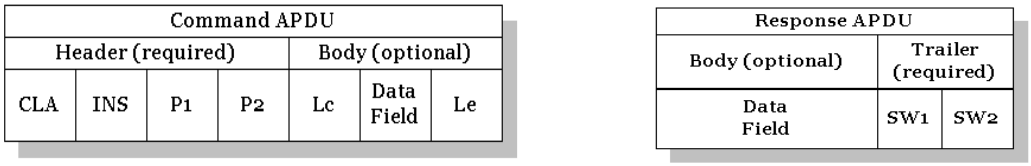

Figura 2: Comando APDU y Respuesta APDU [2]

Los comandos APDU se componen de cabecera y cuerpo. La cabecera está formada por cuatro campos obligatorios que ocupan 1 byte cada uno.

- *CLA:* código de clase. Típicamente 0x80.

- *INS:* determina la instrucción a ejecutar. Hay campos INS estandarizados para realizar diversas funciones de GlobalPlatform o ISO/IEC 7816, pero pueden tener cualquier valor en nuestra aplicación específica.
- *P1 y P2:* son los campos reservados para estableces diferentes opciones para una misma instrucción

El cuerpo se divide en tres campos, dos de un byte u uno de longitud variable:

- *Lc:* determina la longitud del campo de datos.
- *Data:* son los datos a enviar, si los hubiere.
- *Le:* el número de bytes que se espera recibir en la respuesta

Las respuestas APDU constan de cuerpo y un tráiler. En este caso se coloca primero el cuerpo, si existe, y posteriormente se coloca el tráiler con los códigos de respuesta

- *Data:* datos a enviar en la respuesta
- *SW1 y SW2:* conforman el código de respuesta.

Actualmente la última versión de JavaCard es la 3.0.4, la cual proporciona todos los aspectos básicos de JavaCard además de funcionalidad extendida que abarca la creación de "servlets" y aplicaciones más sofisticadas con conexión a Internet.

Sin embargo, la versión empleada a lo largo de todo el transcurso de las prácticas es la 2.2, la cual presenta algunas mejoras importantes respecto a la 2.1.1 y además incorpora funcionalidades nuevas tales como los servicios globales.

3.1.5 GlobalPlatform

GlobalPlatform proporciona toda la funcionalidad necesaria para administrar el contenido de una tarjeta JavaCard de forma segura. En el estándar se recogen aspectos relacionados con la instalación, borrado y gestión de "applets", así como diferentes

estructuras para proporcionar seguridad adicional en nuestras aplicaciones frente a amenazas.

GlobalPlatform define que una tarjeta JavaCard está dividida en varios bloques llamados dominios de seguridad, entre los cuales se encuentra el dominio de seguridad del fabricante, más conocido por sus siglas en inglés, ISD. El ISD es el dominio por defecto y el que tiene todos los privilegios para la administración de la tarjeta. Cada dominio de seguridad puede albergar ninguno, uno o varios "applets" JavaCard y pueden estar jerarquizados, es decir, un dominio de seguridad puede estar dentro de otro.

Al igual que los contextos en JavaCard, una tarjeta GlobalPlatform dispone de firewalls para proteger la información contenida en ella. De este modo las aplicaciones pertenecientes a un dominio de seguridad no pueden acceder a la información de otro dominio a no ser que disponga de los permisos necesarios (*véase "Figura 3: Security Domains GP"*).

Figura 3: Security Domains GP [3]

Como se ha dicho anteriormente, GlobalPlatform proporciona una plataforma de seguridad (gracias a los dominios de seguridad y firewalls) y administración. Gracias a GlobalPlatform podemos administrar el contenido de una tarjeta JavaCard mediante comandos. Los comandos más comunes son aquellos que nos permiten realizar operaciones como autenticarnos en un dominio, cargar un "applet" en la tarjeta, instalarlo, borrarlo o enviarle nuestros propios comandos encriptados para obtener la funcionalidad deseada de nuestra aplicación.

Además de esto tenemos comandos para ver el contenido de la tarjeta, mostrar información acerca de ella, almacenar datos o incluso introducir nuevas claves de acceso para un dominio en concreto.

3.2 NFC

NFC (*Near Field Communication*) es una tecnología inalámbrica de corta distancia y alta frecuencia empleada para la transmisión de pequeñas cantidades de datos entre dispositivos. Actualmente la tecnología NFC está empezando a ser implementada en dispositivos móviles debido a su gran utilidad, no sólo para la transferencia de archivos, sino para otras muchas aplicaciones como, por ejemplo, la posibilidad de hacer "bluetooth pairing" de una forma rápida y sencilla o la posibilidad de hacer funcionar nuestro teléfono móvil como una tarjeta inteligente.

3.2.1 Orígenes y tecnología RFID

NFC se basa en tecnología de radiofrecuencia RFID, empleada principalmente para intercambiar pequeñas cantidades de información, típicamente un número de serie o un identificador, entre un lector y una etiqueta o "tag".

Las etiquetas o "tags" son unos pequeños dispositivos en forma de tarjeta o pegatina que contienen una antena capaz de recibir y enviar información al lector RFID. Estos "tags" pueden ser, según la norma, de dos formas:

- Activos: Poseen una fuente de alimentación que utilizan para modular y enviar información al receptor. Son capaces de iniciar una comunicación inalámbrica. Permiten una comunicación a mayor distancia.

- Pasivos: No constan de fuente de alimentación por lo que emplean la energía procedente de la señal del lector para generar las señales se respuesta. Al contrario que los "tags" activos, no pueden iniciar una comunicación ya que no disponen de fuente de energía.

Existen muchos tipos de "tags" RFID, cada uno empleado en unos sectores y para unas aplicaciones específicas. El precio puede variar dependiendo de la frecuencia que estemos empleando, la velocidad de transmisión, el tipo etc.

3.2.1.1 Estándar ISO/IEC 14443

Dentro de la amplia tecnología RFID podemos destacar las denominadas "tarjetas de proximidad", las cuales se encuentran estandarizadas en la norma ISO/IEC 14443. La tecnología NFC se basa principalmente en este estándar y presenta algunas características adicionales.

Las tarjetas o "tags" de proximidad emplean una tecnología inalámbrica a una frecuencia de 13.56 MHz y unas velocidades de transmisión que varían dependiendo del tipo de tarjeta y de los propósitos de nuestro sistema. Existen varios tipos de tarjeta dentro del estándar ISO/IEC 14443: de tipo A y de tipo B. Ambos tipos se diferencian en aspectos tales como la modulación, esquemas de codificación y velocidades de transmisión, entre otras cosas, aunque los dos tipos emplean el mismo protocolo de transmisión, denominado T=CL.

Este estándar se divide en 4 partes bien diferenciadas:

- ISO/IEC 14443-1: Características físicas
- ISO/IEC 14443-2: Interfaz radio
- ISO/IEC 14443-3: Inicialización y anticolisión
- ISO/IEC 14443-4: Protocolo de transmisión

Existen numerosas implementaciones parciales de este estándar como por ejemplo en las tarjetas MIFARE (ISO/IEC 14443-3A) o Calypso (ISO/IEC 14443-3B), las

cuales utilizan su propio protocolo de transmisión (no disponen del protocolo T=CL) en sus comunicaciones.

3.2.2 Características

Como se ha comentado antes, la tecnología NFC está basada en la tecnología RFID, pero, ¿qué diferencias hay entre una y otra?. Inicialmente NFC se define en el estándar ISO/IEC 18092 (NFCIP-1) y en él se recogen todas las características y especificaciones necesarias para implementar la tecnología inalámbrica en dispositivos móviles tales como smartphones o tabletas, mientras que la tecnología RFID (nos centraremos en la ISO/IEC 14443) abarca el ámbito de las tarjetas inteligentes.

Al igual que el ISO/IEC 14443, la tecnología NFC opera a una frecuencia de 13.56 MHz (dentro de la banda ISM) y alcanza unas velocidades de transmisión que pueden oscilar entre 106, 212 o 424 kbps. El sistema de codificación empleado varía de acuerdo a la velocidad de transmisión y el tipo de "tag" (activo o pasivo) (*véase "Tabla 1: Relación de velocidades y codificaciones").*

Tabla 1: Relación de velocidades y codificaciones

Velocidad	Modo Activo	Modo Pasivo
424 kbps	Codificación: Manchester Modulación: ASK Índice modulación: 0,1	Codificación: Manchester Modulación: ASK Índice modulación: 0,1
212 kbps	Codificación: Manchester Modulación: ASK Índice modulación: 0,1	Codificación: Manchester Modulación: ASK Índice modulación: 0,1
106 kbps	Codificación: Manchester Modulación: ASK Índice modulación: 1	Codificación: Manchester Modulación: ASK Índice modulación: 0,1

Existen varios tipos de "tags" NFC estandarizados por el NFC Forum que funcionan con cualquier tipo de dispositivo de estas características. Estos "tags" están basados principalmente en la norma ISO/IEC 14443 A o B, debido a la estrecha relación técnica entre este estándar y la tecnología NFC. A continuación se comentan las principales características de los diferentes tipos (*véase "Tabla 2: Tipos de tag NFC Forum "*):

- Tipo 1 y Tipo 2: presentan poco espacio de almacenamiento
- Tipo 3: presenta gran espacio de almacenamiento y una gran seguridad, pero son muy costosos.
- Tipo 4: presentan un almacenamiento considerable, suficiente para la mayoría de las aplicaciones, pero su método de encriptación es inseguro y por tanto, en algunas aplicaciones que requieran seguridad, no merece la pena el coste a pagar.

Tabla 2: Tipos de tag NFC Forum [4]

NFC FORUM TYPE	POPULAR PRODUCTS OF THIS TYPE	OPERATIONS SPECIFICATIONS	REWRITE CAPABILITIES	AVAILABLE MEMORY	COMMUNICATION SPEED	PRICE RANGE (PRICE PER UNIT)
1	Broadcom Topaz	ISO 14443A	User rewrit-able; can be marked as read-only by user	96 bytes, expand-able to 2KB	106kbit/s	Low (~$1-2 USD)
2	MIFARE UltraLight	ISO 14443A	User rewrit-able; can be marked as read-only by user	48 bytes, 144 bytes is com-mon, expand-able to 2KB	106kbit/s	Low (~$1-2 USD)
3	Sony FeliCa	JIS X 6319-4	Manufacture pre-config-ured to be read-only or re-writable.	variable, theoreti-cal 1MB	212kbit/s or 424kbit/s	High (~$8-10 USD or higher)
4	NXP DESFire, NXP SmartFX	ISO 14443A, ISO 14443B	Manufacture pre-config-ured to be read-only or rewritable.	4KB for DESFire, up to 32KB for SmartFX	Up to 424kbit/s	Medium-High (~$3-4 USD)

Teóricamente la distancia máxima de funcionamiento de un "tag" NFC es de unos 10 cm pero la realidad es que los dispositivos NFC necesitan estar más cerca para poder establecer la comunicación.

3.2.3 Estandarización

La estandarización de la tecnología NFC conlleva la agrupación de los tres estándares descritos a continuación (*véase "Figura 4: Estándar NFC"*):

- ISO/IEC 18092 (NFCIP-1): Recoge el estándar puramente de NFC. Se incluyen todos los aspectos técnicos de la interfaz NFC y el protocolo para la comunicación entre dos dispositivos.
- ISO/IEC 14443: En este estándar se recogen todos los aspectos referentes a las tecnologías RFID de campo cercano. Incluye las especificaciones de las llamadas "tarjetas de proximidad".
- ISO/IEC 15693: Son las denominadas "tarjetas de vecindad". Son muy parecidas a las tarjetas de proximidad (ISO/IEC 14443) con la salvedad de que pueden operar a una mayor distancia.

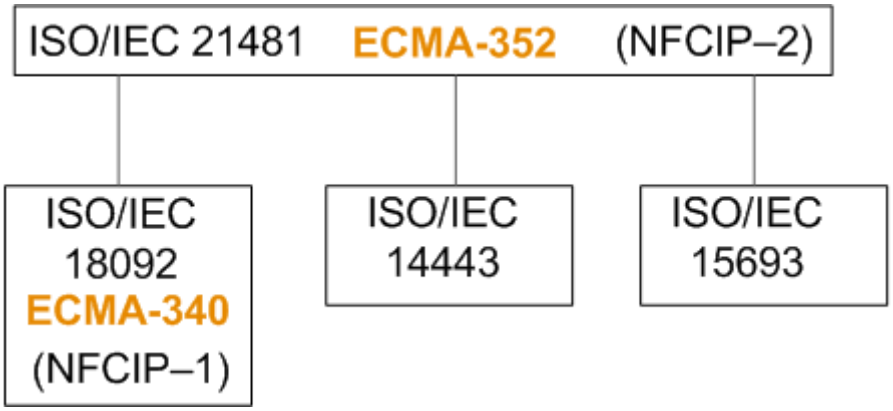

Figura 4: Estándar NFC [5]

Todos estos estándares se recogen bajo el ISO/IEC 21481 (NFCIP-2), el cual establece los mecanismos de selección necesarios en un dispositivo compatible con estas tres tecnologías. Proporciona una manera de unificar las comunicaciones inalámbricas de este tipo y de realizar la selección de la tecnología necesaria en cada momento de forma automática.

3.2.4 Modos de funcionamiento

Existen tres modos de funcionamiento para un dispositivo NFC (*véase "Figura 5: Modos NFC"*):

- *Modo lectura/escritura:* En este modo, un dispositivo móvil es capaz de leer la información contenida en un "tag" NFC y escribir información en él. Este modo es ampliamente utilizado, por ejemplo, es los llamados SmartPosters. Los SmartPosters son unos "tags" NFC a modo de pegatina que contienen información relevante sobre algún tema en concreto. De este modo, para extraer dicha información, un usuario no tiene más que acercar su dispositivo móvil y leer el "tag". De igual forma, mediante este modo de funcionamiento se puede escribir información en un SmartPoster con sólo acercar el dispositivo.

- *Modo Peer-to-Peer:* Este modo de funcionamiento consiste en el intercambio de pequeñas cantidades de información vía NFC entre dos dispositivos móviles, tales como dos smartphones. Para este modo de funcionamiento es necesario el uso del protocolo LLCP (*Logical Link Control Protocol*), el cual permite una comunicación bidireccional entre dos dispositivos NFC. Este modo puede ser útil para intercambiar pequeñas cantidades de datos entre dos teléfonos o para realizar funciones como el *Bluetooth pairing* de una manera rápida y eficaz.
- *Modo "card emulation":* Este modo es quizás el más útil de los tres y en el que nos vamos a centrar en este proyecto, ya que permite que un dispositivo móvil pueda actuar como un "tag" NFC gracias a un SE (*Secured Element*) incluido en el terminal (tarjetas de memoria externa y la propia tarjeta SIM). Este modo de funcionamiento tiene numerosas aplicaciones importantes como por ejemplo la posibilidad de efectuar pagos mediante nuestro teléfono móvil haciendo uso de la tecnología NFC.

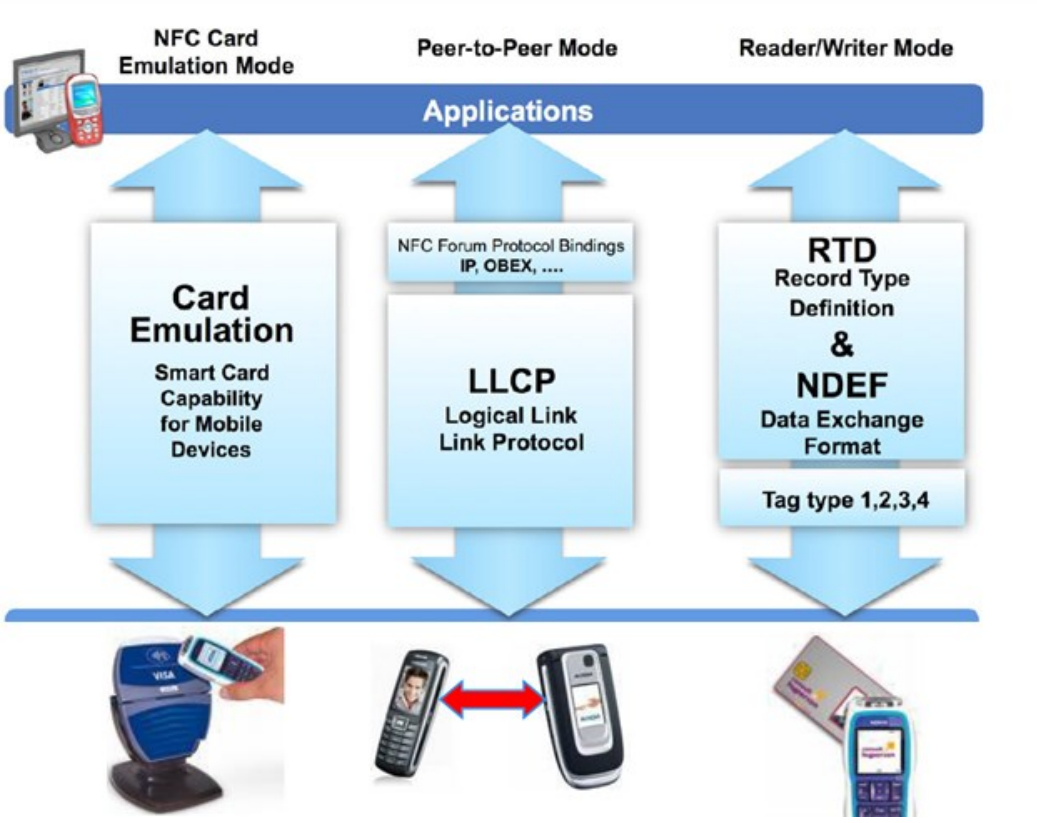

Figura 5: Modos NFC [6]

3.2.5 Formato de los mensajes

En NFC el formato más ampliamente utilizado para el intercambio de mensajes es el denominado NDEF (*NFC Data Exchange Format*) ya que se encuentra estandarizado por el NFC Forum y presenta una forma sencilla de organizar la información presente en las comunicaciones.

El formato NDEF se compone de varios conjuntos de datos llamados NFCRecords, los cuales constituyen la unidad básica de información en un mensaje. A su vez, cada NFCRecord contiene varios campos bien diferenciados con información referente al tamaño del mensaje, el contenido, el tipo y un identificador (*véase "Figura 6: Mensaje NDEF"*).

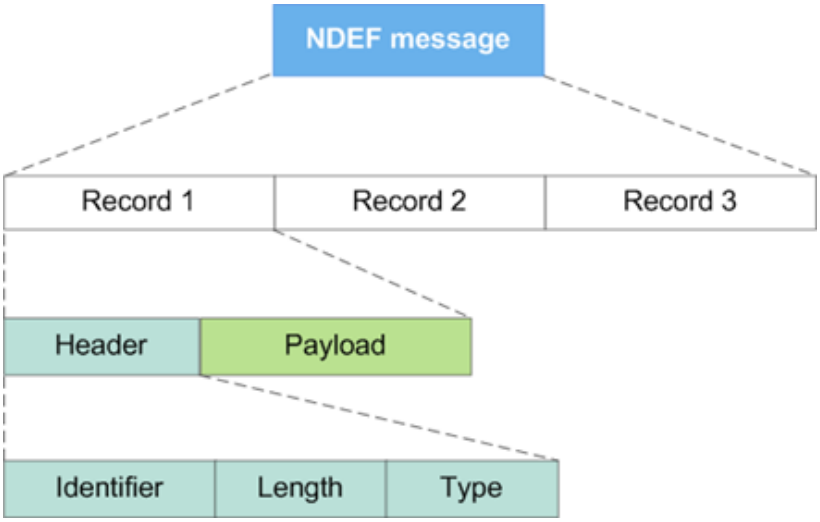

Figura 6: Mensaje NDEF [7]

3.2.6 Implicaciones de seguridad

La seguridad en un sistema que emplee la tecnología NFC es muy importante debido a la propia naturaleza insegura de las transmisiones inalámbricas. A pesar de que NFC presenta una comunicación a muy corta distancia (teóricamente 10 cm) haciendo más difícil el acceso a información de manera fraudulenta, existen mecanismos que

permiten poner en entredicho un sistema de estas características. Los ataques más comunes son los siguientes:

- *Sniffing o eavesdropping:* Técnica empleada por el atacante para escuchar la comunicación entre dos dispositivos comunicándose mediante NFC. Esta técnica está muy limitada por la distancia y depende en gran medida de si el afectado está empleando un dispositivo activo o pasivo. La solución a este ataque es la de emplear un canal seguro en las comunicaciones.
- *Corrupción de datos:* Se trata de un ataque DoS (Denial os Service) empleado para interrumpir la comunicación entre dos dispositivos NFC. Este tipo de ataque es detectable ya que la tecnología NFC permite escuchar a la vez que se transmiten datos detectando así posibles colisiones.
- *Modificación de los datos:* Es similar a la corrupción de datos pero en este caso se mantiene la validez de los mismos, es decir, únicamente se modifican haciéndose fraudulentos. Presenta mayor o menor dificultad de realización dependiendo de la codificación que se esté empleando en la comunicación. Si se emplea una codificación Miller en el 100% de profundidad de modulación será más difícil realizar acciones malignas en los datos ya que sólo se pueden modificar los bits que sean "1" y vayan seguidos de otro "1", mientras que si la codificación empleada es la Manchester con un 10% de profundidad de modulación, cualquier bit puede ser modificado.
- *Man In The Middle:* Es un ataque típico que consiste en "ponerse en medio" de una comunicación entre dos máquinas teniendo la posibilidad de comunicarse con ambas, sin que se enteren los interlocutores originales.

3.2.7 NFC en tarjetas inteligentes

Como se mencionó en apartados anteriores, existen tarjetas SIM que hacen uso de uno de sus pines metálicos para establecer una comunicación serie con el chip NFC de

un teléfono móvil o dispositivo similar y así poder intercambiar información con el exterior de forma inalámbrica.

Este tipo de tarjetas está empezando a proliferar entre las operadoras de telefonía móvil más importantes para ofrecer ciertos servicios tales como pagos mediante NFC, servicios de almacenamiento de tickets en el móvil etc. Todo ello gracias al modo "card emulation" antes mencionado.

Para conseguir este modo de funcionamiento, la tarjetas y el chip NFC emplean un protocolo estandarizado por ETSI denominado SWP (*Single Wire Protocol*). Este protocolo hace uso del pin C6 de la tarjeta inteligente para comunicarse con el chip NFC y así poder establecer comunicación con el exterior sin pasar por el sistema operativo del móvil en cuestión. De esta forma, un usuario puede realizar, entre otras cosas, una transacción empleando su tarjeta SIM como un monedero electrónico o como una tarjeta de débito asociada con su banco, incluso con el móvil apagado.

3.2.7.1 SWP/HCI

SWP es un protocolo orientado a bit que sirve para establecer una comunicación entre un UICC (*Universal Integrated Circuit Card*), en nuestro caso una SIM, y el CLF (*Contactless Frontend*), o chip NFC de un dispositivo móvil. Este protocolo constituye el nivel de enlace de un sistema de estas características, mientras que el protocolo HCI (*Host Controller Interface*) proporciona una interfaz entre hosts para realizar las comunicaciones.

HCI se fundamenta en el uso de estructuras de datos llamadas gates (puertas), pipes (tuberías) y registries (registros) para controlar la comunicación entre el CLF y la UICC. La forma de comunicación se realiza mediante comandos y respuestas, pero la especificación detallada de estos elementos está más allá de los límites de este TFG.

3.3 Biometría

En este apartado se hará una pequeña introducción a la biometría. Asimismo se comentarán algunas de las características principales de los sistemas de reconocimiento biométrico y algunos parámetros importantes empleados en la verificación de personas. Finalmente se hará una breve introducción a la modalidad de iris, empleada en este TFG.

3.3.1 Introducción

La biometría consiste en el estudio de métodos automáticos de reconocimiento de humanos mediante sus rasgos físicos y de comportamiento. Existen numerosas modalidades biométricas, es decir, numerosos rasgos físicos y de comportamientos únicos en los seres humanos que permiten identificarlos de forma unívoca. Entre las modalidades más utilizadas podemos encontrar huella dactilar, iris, reconocimiento facial, reconocimiento vascular de la mano, retina, reconocimiento de voz, firma manuscrita o incluso ADN.

Para poder construir un sistema de reconocimiento biométrico hay que tener en cuenta dos fases para la autenticación de una persona:

1. *Reclutamiento:* Consiste en extraer un muestra del rasgo físico en cuestión, dependiendo de la modalidad biométrica, para registrar a un usuario en el sistema con su información única. Esta operación se lleva a cabo a través de un dispositivo biométrico que examina el atributo físico o de comportamiento y, a través de operaciones matemáticas y estadísticas, extrae un patrón que representa unívocamente al usuario.
2. *Reconocimiento:* Consiste en extraer nuevamente un patrón del rasgo físico para compararlo con el que hay almacenado en el sistema y poder decidir si el usuario es quien dice ser o no.

Para que la autentificación se lleve de modo correcto, no necesariamente ambos patrones deben coincidir. Como se comenta a continuación, no siempre se va a realizar la misma medida.

Naturalmente no todas las características biológicas son adecuadas para una identificación biométrica. Tienen que cumplir los siguientes requisitos para poder llevar a cabo el proceso:

- Que pueda ser medida eficazmente (en términos del método de medida, tiempo y coste)
- Que se pueda asociar de manera inequívoca a un usuario.
- Que no pueda ser alterada.
- El patrón generado debe ser pequeño (100~1000 bytes)

Como sucede al realizar cualquier proceso de medida, el resultado de cada "muestra" no es exactamente igual al anterior, sino que varía de muestra a muestra. Con un método ideal de medida y una cualidad biométrica también ideal, no existe variación en las medidas y la curva de dispersión se ve reducida a una línea vertical. Pero en realidad, esta curva se aproxima más a una curva gaussiana como se puede apreciar en la siguiente figura.

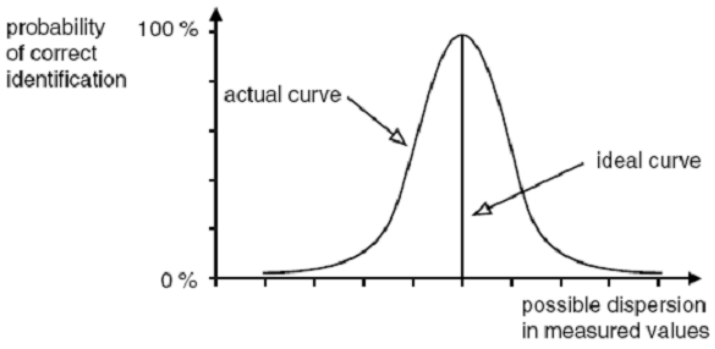

Figura 7: Distribución de probabilidad para repetidas medidas biométricas

Si se parte de la anterior figura y se añade otra curva similar correspondiente a otro sujeto, se obtiene una representación como la mostrada en la Figura 8. La curva adicional representa una medida que está tan cerca de la original como para afectar en la decisión de identificación. En el punto de intersección existe la misma probabilidad de que una persona sea correctamente identificada o no. Por lo tanto en los sistemas biométricos se define un valor mínimo que debe superar la muestra para poder tomar como correcta la identificación. El valor de la Figura 8 nos muestra cuatro posibles regiones distintas.

Los parámetros básicos para evaluar un sistema biométrico son, la Tasa de Falsa Aceptación (FAR) y la Tasa de Falso Rechazo (FRR). La FAR es la probabilidad de permitir el acceso a personas no autorizadas, mientras que la FRR es la probabilidad de rechazo de personas autorizadas. Lógicamente estas dos probabilidades no pueden ser elegidas libremente, ya que están definidas por el método biométrico. Además, FAR y FRR están ligadas entre sí, una Tasa de Falsa Aceptación baja conlleva una Tasa de Falso Rechazo alta y viceversa.

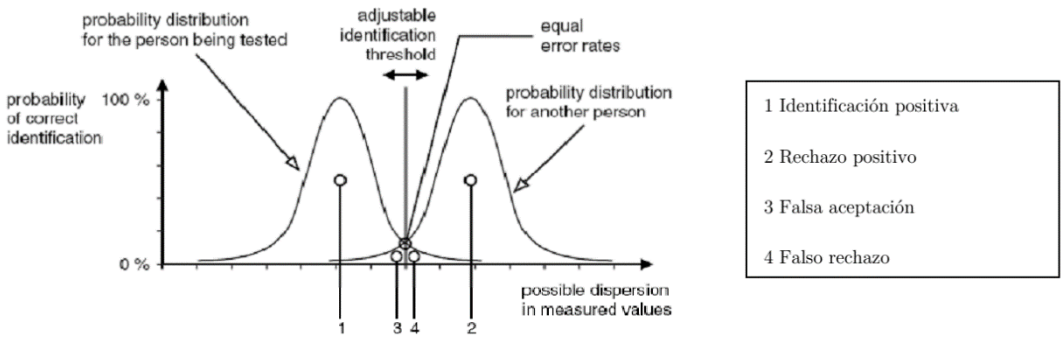

Figura 8: Funciones de probabilidad de una identificación biométrica

3.3.2 Reconocimiento por Iris

El iris constituye una membrana circular de color que sirve para regular la cantidad de luz que penetra en el ojo. Al igual que otras muchas partes del cuerpo, el iris puede emplearse en sistemas de reconocimiento biométrico debido a que posee patrones únicos en cada individuo, producto de la degeneración que sufre cada persona antes del nacimiento.

Para la realización del reconocimiento biométrico mediante iris existen varias operaciones, detalladas a continuación:

- *Captura de la imagen:* consiste en la fotografía de la imagen del ojo en cuestión. Habitualmente esta fotografía está tomada con una cámara de infrarrojos de alta resolución.
- *Pre-procesado:* consiste en eliminar la parte inservible de la imagen capturada, es decir, quedarnos sólo con el iris. En esta parte de procesado de la imagen también se incluye el ecualizado de la fotografía para conseguir hacer una mejor diferenciación de los surcos presentes en el iris.
- *Extracción de características:* Consiste en extraer la información del iris convertida en forma de una secuencia de bits. Esta operación se puede realizar de numerosas formas pero la más empleada es la obtenida mediante los llamados filtros Gabor. El filtrado Gabor consiste en extraer la información de los surcos del iris en base a la anchura y la orientación del filtro.
- *Comparación:* la comparación de los patrones de iris se realiza empleando la distancia de Hamming entre las dos muestras. Adicionalmente se hace uso de una máscara que nos da la información de la situación exacta del iris, dada su forma esférica ligeramente achatada.

3.4 Android

En el siguiente apartado se hará una pequeña introducción al sistema operativo Android empleado en el desarrollo de este TFG, así como a las Open Mobile APIs, las cuales constituyen la base fundamentas en las comunicaciones entre un teléfono móvil y su tarjeta SIM .

3.4.1 Introducción

Android es un sistema operativo basado en Linux y diseñado principalmente para dispositivos móviles fundado por la OHA (*Open Handset Alliance*), la cual está formada por varias compañías entre las que destaca Google. Inicialmente el sistema fue creado por Android Inc. el cual Google respaldó económicamente y finalmente compró en 2005. El sistema operativo Android es un software de código abierto y se puede descargar en Internet de forma totalmente gratuita.

Inicialmente el sistema operativo Android se pensó para ser utilizado en dispositivos móviles tales como smartphones o tabletas pero más adelante se fue exprimiendo el potencial del sistema llegando incluso a ser implementado en televisiones y demás dispositivos del hogar.

De cara al desarrollo, Android proporciona a los desarrolladores una forma fácil e intuitiva de programar ya que se ofrecen las ventajas del lenguaje Java para construir la lógica de las aplicaciones y la simplicidad del lenguaje de marcado XML para construir la apariencia gráfica. Por esto, este sistema está teniendo una gran aceptación en la sociedad y continúa creciendo atrayendo cada vez más y más cuota de mercado.

3.4.2 Versiones

Desde sus inicios en el mercado de los aparatos móviles, Android ha ido sacando nuevas versiones con nuevas funcionalidades y mejoras en la experiencia de usuario (*véase "Figura 10: Versiones Android OS " Y "Figura 9: Cuota de mercado Android OS "*).

Figura 10: Versiones Android OS [8]

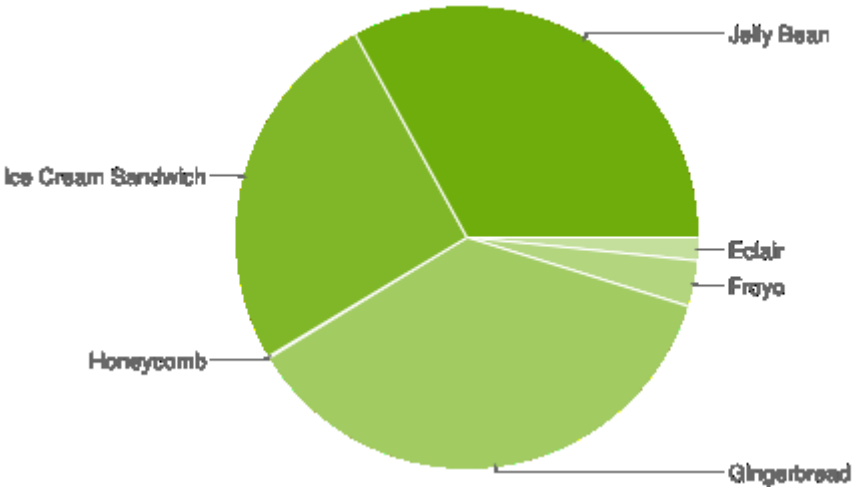

Figura 9: Cuota de mercado Android OS [9]

3.4.3 NFC en Android

A partir de la versión 2.3.3 de Android se incluye parte de la funcionalidad NFC para los dispositivos móviles con esta tecnología, y por tanto, se incluye un API (*Application Programming Interface*) para los desarrolladores que deseen crear

aplicaciones con estas funcionalidades. No es hasta la versión 4.0 (API 14) cuando se incluyen todas las características NFC y todos los modos de funcionamiento descritos en el apartado 3.2.4 de esta memoria.

Las APIs de Android NFC proporcionan un mecanismo sencillo y completo para poder enviar y recibir mensajes, ya sean NDEF o no, entre dispositivos (teléfonos móviles o tarjetas inteligentes). Mediante un dispositivo Android con NFC se puede establecer comunicación con casi cualquier "tag" o terminal móvil que siga las especificaciones ISO/IEC 14443 e ISO/IEC 18092.

3.4.4 Open Mobile APIs

Las Open Mobile APIs son un conjunto de interfaces de programación estandarizadas por SIMAlliance que sirven para proporcionar acceso a un elemento seguro tal como una tarjeta SIM o una tarjeta de memoria SD desde el sistema operativo de un móvil. Gracias a estas APIs podemos enviar comandos ADPU a la tarjeta SIM y recibir respuestas de cualquier applet que tengamos instalado.

Esta APIs proporcionan unas interfaces de comunicación básicas con el elemento seguro para cualquier sistema operativo pero existen implementaciones para los diferentes sistema móviles que podemos encontrar hoy en día. En caso del sistema Android, que es el que vamos a emplear en el ámbito de este TFG, encontramos las denominadas Secure Element Evaluation Kit APIs (*SEEK APIs*). Mediante estas APIs podemos acceder a los elementos seguros de un dispositivo móvil con sistema Android, con el único requisito de que dicho dispositivo sea compatible con las Open Mobile APIs.

El funcionamiento de las SEEK APIs es muy sencillo. Lo más importante son las tres funciones descritas a continuación:

- *Readers[] getReaders:* Obtiene un array de todos los elementos seguros presentes en el dispositivo móvil.
- *Session openSession:* abre una sesión con uno de los elementos seguros obtenidos de la anterior función.

- *Channel openLogicalChannel(byte[] AID):* se abre un canal lógico con uno de los applets presentes en el elemento seguro mediante el envío del comando SELECT junto con el AID del applet que queremos seleccionar.
- *byte[] transmit(byte[] APDU):* esta función es la más importante de todas. Sirve para enviar un comando APDU al elemento seguro. La función retorna un array de bytes con la respuesta recibida.

4. CONTENIDO DEL TRABAJO

4.1 Introducción

Las tarjetas de identificación son actualmente algo habitual en nuestra sociedad, ya que nos proporcionan un medio cómodo y seguro de realizar transacciones en nuestro día a día. El uso de las tarjetas de débito y de crédito está tan extendido que no nos hemos planteado si existe la posibilidad de emplear otro medio aún más cómodo y seguro para realizar nuestras compras y operaciones habituales.

Hoy día, y gracias al gran auge de los teléfonos móviles y las comunicaciones inalámbricas, tales como Wi-Fi o la propia red GSM, se está planteando cada vez más emplear nuestro propio teléfono móvil como tarjeta de débito o simplemente como monedero electrónico. Pero, ¿realmente puede conseguirse esto? Gracias a la reaparición de la tecnología NFC, sí.

Mediante la tecnología inalámbrica de corto alcance NFC podemos conseguir realizar transacciones de una manera fácil y sencilla con sólo acercar nuestro teléfono móvil a un punto de venta NFC. De esta manera, sólo nos hace falta nuestro teléfono móvil para disfrutar de nuestras compras de manera rápida. Con la tecnología NFC podemos realizar transacciones de forma inalámbrica, pero, ¿es esto inseguro? ¿Están mi información personal y mis datos bancarios al alcance de cualquiera? ¿También se transmiten de forma inalámbrica? La respuesta es no, ya que todas las operaciones se realizan en nuestro propio teléfono, más concretamente en nuestra tarjeta SIM, la cual cuenta con unos mecanismos de seguridad excelentes e infranqueables por un agente externo.

Figura 11: Pago con NFC [10]

Gracias a la aparición de las tarjetas SIM NFC somos capaces de realizar dichas transacciones de forma inalámbrica en su interior, es decir, nuestra SIM es nuestra tarjeta de débito, crédito o monedero electrónico.

Así pues, y siguiendo las premisas aquí mencionadas, lo que se pretende en este trabajo de fin de grado es diseñar y construir un sistema de pagos inalámbrico NFC que cumpla con los requisitos de seguridad que demanda cada vez más la sociedad y que presente una forma fácil e intuitiva de realizar nuestras operaciones financieras más habituales.

4.2 Objetivos

El principal objetivo de este proyecto es su presentación como TFG (trabajo de fin de grado), pero más allá de este ámbito, existen una serie de objetivos no menos importantes:

1. Simplificar las operaciones de compra mediante dispositivos electrónicos
2. Aumentar la seguridad en las transacciones inalámbricas

3. Añadir un mecanismo más robusto de autenticación del titular del teléfono, como es el caso del reconocimiento biométrico.

4.3 Alcance

El alcance de este proyecto comprende la creación de un sistema de pagos electrónico mediante el uso de la tecnología inalámbrica NFC. Se emplearán dos dispositivos móviles NFC, uno de ellos actuando como cliente y otro como punto de venta. Por tanto, para la realización de este sistema son necesarios los siguientes elementos:

- *Punto de venta (POS):* Se trata del terminal que ofrece los productos al usuario. Un punto de venta podría ser una máquina expendedora o un terminal de venta en una tienda de ropa.
- *Terminal cliente:* Es el teléfono móvil personal del usuario y constituye un centro de aplicaciones y servicios. Es el dispositivo que utilizará el usuario para pagar los productos que compre.
- *Tarjeta SIM NFC:* Es la tarjeta SIM alojada en el terminal móvil del usuario que nos proporciona los servicios de conexión a la red móvil, entre otros. Esta tarjeta será la que nos proporcione un servicio de almacenamiento de fondos que el usuario contratará con su banco.

Así pues, el alcance de este TFG se reduce a realizar la implementación de los siguientes componentes de software:

- Aplicación para el punto de venta que permita seleccionar productos y proporcione una interfaz de pago.
- Aplicación para el terminal móvil del cliente que permita al usuario conocer su saldo disponible y le permita autenticarse.

- Aplicación para la tarjeta SIM que realice las funciones de un servicio bancario, ya sea monedero electrónico, tarjeta de débito o crédito, o cualquier otra función.

4.4 Requisitos

A continuación se expone la relación de requisitos impuestos para el diseño del sistema:

- La aplicación del punto de venta será una aplicación Android que simule el software de una máquina expendedora de bebidas, es decir, el usuario será capaz de escoger una bebida entre todas las disponibles y pagarla mediante su teléfono móvil.
- La aplicación del terminal móvil del cliente será para el sistema operativo Android y será capaz de ofrecer al usuario la siguiente funcionalidad:
    - Consultar su saldo
    - Ingresar fondos
    - Autenticarse
    - Reclutar sus datos biométricos
- Se debe implementar autenticación biométrica con iris
- Una vez autenticado, el usuario dispondrá de un tiempo limitado para realizar sus compras, finalizado el cual, deberá proceder con una nueva autenticación para continuar realizando sus transacciones.
- La aplicación de la tarjeta SIM NFC será para el sistema operativo JavaCard y hará las funciones de un monedero electrónico, es decir, el usuario será capaz de almacenar dinero en su tarjeta, el cual será totalmente independiente del dinero de su cuenta bancaria, si la hubiere.

4.5 Diseño del sistema

Podemos agrupar los tres elementos de nuestro sistema de transacciones descritos en el apartado 4.3 en dos subsistemas (*véase "Figura 12: Sistema de transacciones NFC"*):

- Sistema servidor: formado por el POS.
- Sistema cliente: está formado por el terminal móvil del cliente y la tarjeta SIM NFC que lleva integrada.

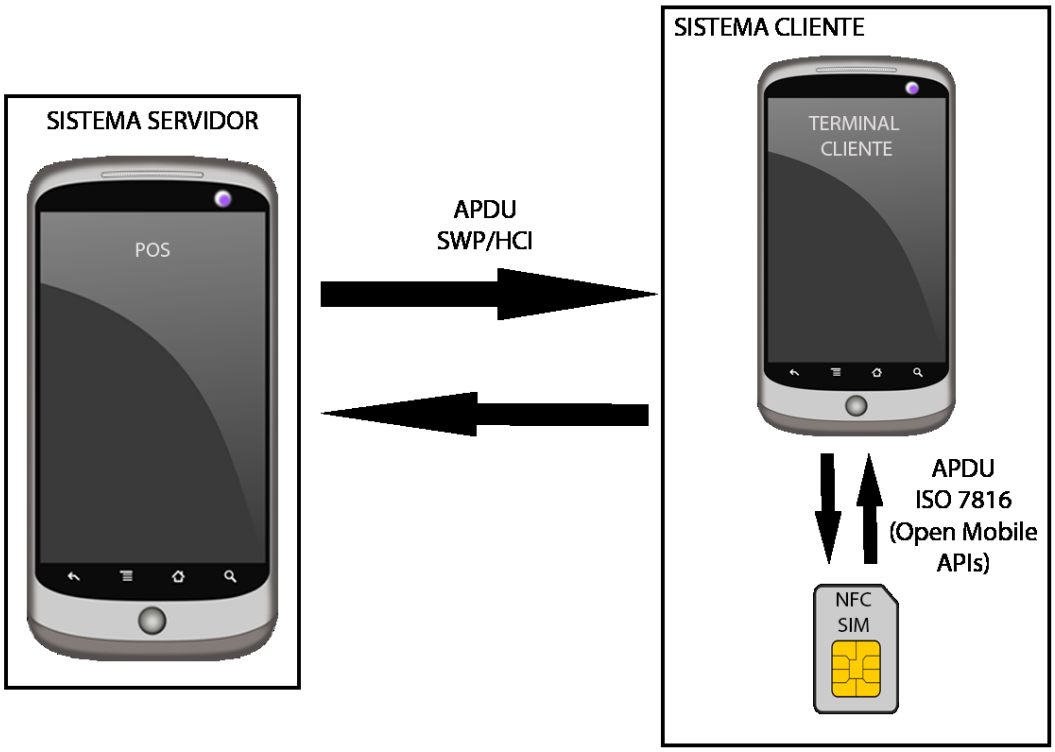

Figura 12: Sistema de transacciones NFC

4.5.1 Sistema servidor

El sistema servidor, tal y como se mencionó anteriormente, está formado por el POS. En el ámbito de este TFG, el POS constituye una máquina expendedora de bebidas, por lo que se ha implementado el software que necesita dicha máquina para comunicarse con el dispositivo móvil del usuario del sistema.

Figura 13: Soft-drink Shop

El software está bautizado como “Soft-drink Shop” y está implementado para el sistema operativo Android. No es más que una interfaz donde aparecen bebidas que el usuario puede seleccionar para su compra mediante su teléfono móvil. En el siguiente apartado se describe en detalle el funcionamiento de la aplicación.

4.5.1.1 Soft-drink Shop

Objetivos

Los objetivos de este software no son más que proporcionar un entorno de pruebas para las aplicaciones NFC en tarjetas inteligentes JavaCard, así como los métodos de autenticación biométrica en el lado del cliente. Este software constituye una forma de probar, simulando un sistema real de máquinas expendedoras, cómo se pueden realizar transacciones con un móvil que contenga una tarjeta SIM NFC y cuáles son los límites y restricciones que suponen.

Alcance

El alcance de esta aplicación es la de proporcionar un sistema de pagos de bebidas mediante la tecnología inalámbrica NFC. Con esto se pretende que un usuario interesado en adquirir un producto, no tenga más que seleccionarlo en la pantalla y acercar su terminal móvil con NFC para realizar el pago de forma segura.

Funcionamiento

El funcionamiento de la aplicación “Soft-drink Shop” es sencillo e intuitivo y propone al usuario una manera amigable de realizar la compra de un producto.

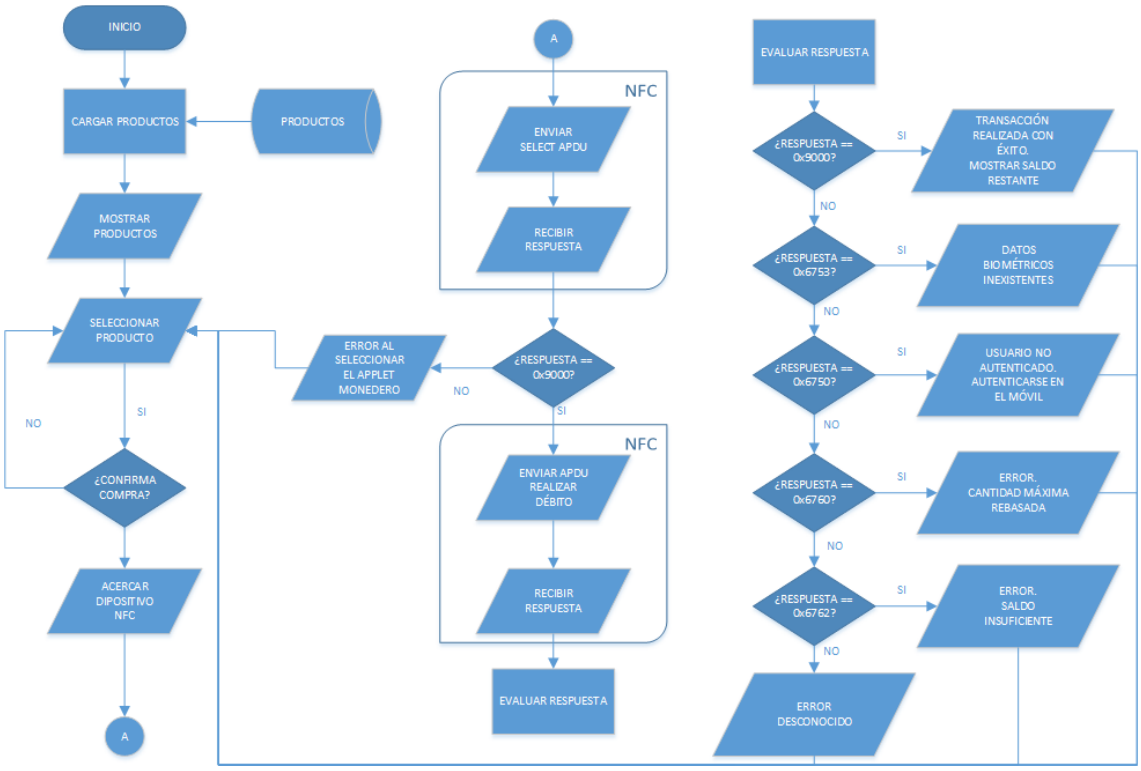

Figura 14: Diagrama de flujo Soft-drink Shop

A continuación se explica en detalle el funcionamiento de la aplicación.

1. Al inicio, el programa accede a una base de datos SQLite almacenada localmente para extraer toda la información sobre los productos que se van a ofertar al cliente.
2. La aplicación muestra por pantalla una lista de todos los productos ofertados que se extrajeron de la base de datos los cuales se muestran en forma de lista en la que el usuario puede hacer "scroll" para seleccionar el más apropiado (*véase "Figura 15: Selección de productos Soft-drink Shop"*).
3. Una vez que el usuario ha seleccionado el producto de su agrado, se muestra una ventana de confirmación para asegurar que el cliente desea proceder con el pago.

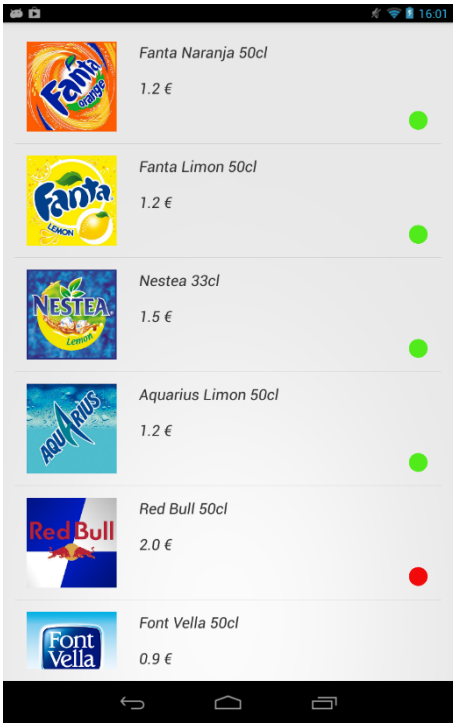

Figura 15: Selección de productos Soft-drink Shop

4. Si el usuario no ha accedido a proceder con el pago, entonces el sistema vuelve a la pantalla con el listado de todos los productos por si es cliente desea realizar otra compra. Por el contrario, si se decidió proceder con el pago, el sistema notificará al cliente de que debe acercar su dispositivo NFC al lector para continuar (*véase "Figura 16: Acercar dispositivo Soft-drink Shop"*).

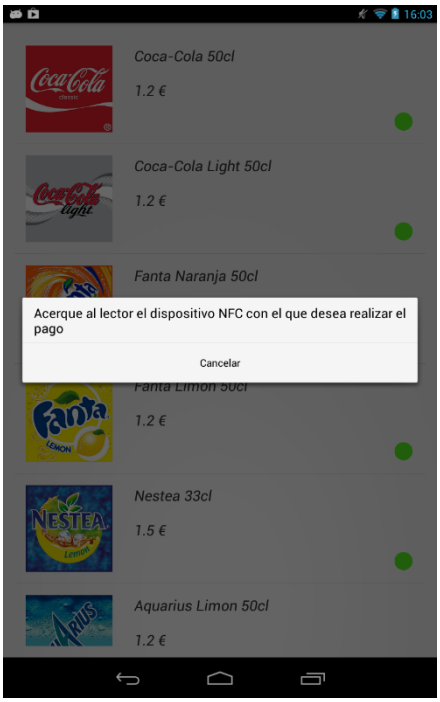

Figura 16: Acercar dispositivo Soft-drink Shop

5. En el momento en que el cliente acerque su terminal móvil al lector y éste lo detecte, el POS enviará un comando APDU de selección para seleccionar el "applet" del monedero electrónico instalado en la tarjeta SIM NFC del cliente. Una vez que se ha recibido y procesado el comando, el terminal cliente enviará una respuesta APDU al POS indicando el resultado. Pueden darse dos casos:
    a. La respuesta es una respuesta de éxito (0x9000) y el "applet" del monedero se ha seleccionado correctamente. En este caso, la aplicación continúa al paso siguiente.
    b. La respuesta es de error (0x6A82) ya que el "applet" no se ha podido seleccionar porque no se encuentra instalado en la tarjeta SIM. En este caso la aplicación muestra su mensaje de error y vuelve a la pantalla de selección de producto.
6. Una vez que se ha seleccionado la aplicación de monedero correctamente, debemos proceder a descontar el importe del producto al saldo total almacenado en el monedero electrónico de la SIM. Para ello, nuevamente el POS manda un comando APDU para efectuar el débito con la información relativa al importe del

producto a la tarjeta SIM del terminal cliente. Una vez que sea recibida y procesada, el cliente mandará una respuesta de vuelta al POS indicando el resultado de la operación. Pueden darse varios casos:

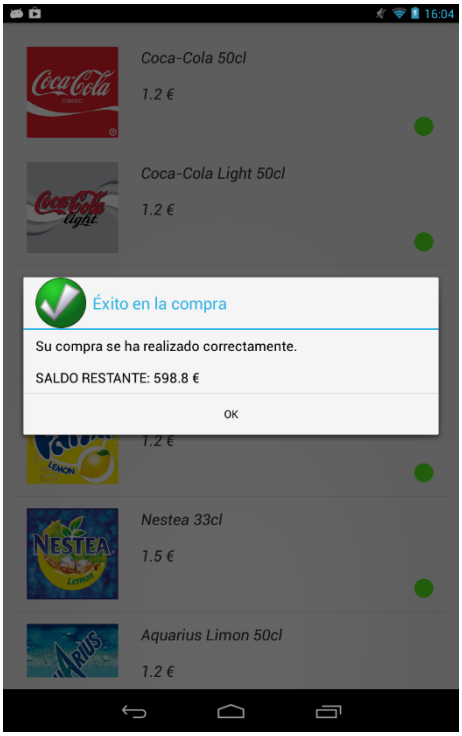

Figura 17: Mensaje éxito Soft-drink Shop

a. El POS recibe una respuesta de éxito (0x9000). En este caso la operación se ha realizado correctamente. El sistema muestra un mensaje de confirmación y el saldo restante del monedero del cliente (*véase "Figura 17: Mensaje éxito Soft-drink Shop").*
b. Se recibe una respuesta que indica que no existen datos biométricos reclutados (0x6753) (*véase "Datos Biométricos No Reclutados"*). En este caso se ha detectado que el usuario no dispone de datos biométricos reclutados en su monedero electrónico. Se muestra un mensaje indicando el error.

c. Se recibe una respuesta de error de autenticación (0x6750) (*véase "Datos Biométricos No Validados"*). En este caso, el "applet" monedero ha detectado que el usuario que intentó hacer la compra no está autenticado, y por tanto no está autorizado para proceder con el pago. Se muestra un mensaje al cliente indicando que se autentique en su dispositivo móvil y que vuelva a intentar la compra (*véase "Figura 18: Datos biométricos no validados Soft-drink Shop"*).

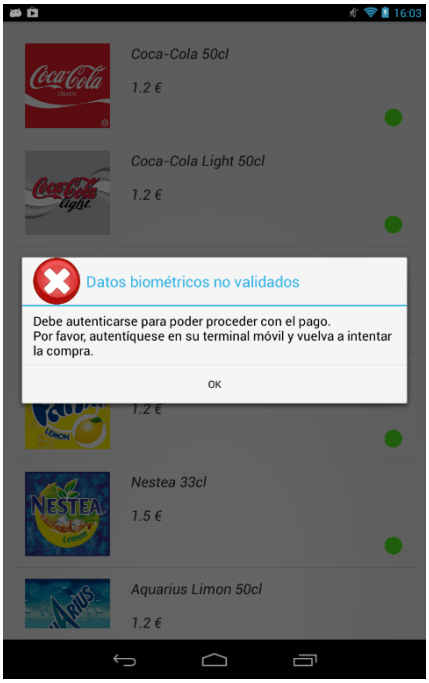

Figura 18: Datos biométricos no validados Soft-drink Shop

d. Se recibe una respuesta de error en la transacción debido a que se ha rebasado la cantidad máxima para un único pago (0x6760) (*véase "Cantidad de Transacción Inválida"*). En tal caso, el sistema muestra un mensaje de error en el que se informa al cliente de lo sucedido y se le recomienda ponerse en contacto con su operador para modificar el límite de pago para una transacción.

e. El POS recibe una respuesta de error en la transacción debido a que no hay suficiente saldo disponible para realizar el pago (0x6762) (*véase "Balance Negativo"*). En este caso se muestra un mensaje de error al

cliente informando de la falta de fondos y recomendándole acudir al punto de recarga más cercano para añadir fondos en su tarjeta.

f. Se recibe un mensaje de error desconocido. En este caso se recibe un mensaje de error no contemplado por el "applet" monedero de la tarjeta SIM. Se muestra un mensaje al usuario indicando que vuelva a realizar la compra y que, si el problema persiste, se ponga en contacto con su operador.

En cualquiera de los casos citados anteriormente el sistema retorna a la pantalla de selección de producto una vez que el usuario ha terminado con su compra.

Posibles mejoras

El software "Soft-drink Shop" está pensado únicamente como medio de prueba en un sistema de pagos NFC mediante la tecnología SWP/HCI en tarjetas SIM de teléfonos móviles. Aun así, este software podría llegar a implementarse en un sistema real de máquinas expendedoras, por lo que se exponen a continuación una lista de posibles mejoras que harían la aplicación mucho más funcional:

1. Añadir la posibilidad de hacer selección de múltiples productos.
2. Añadir la posibilidad de ver los datos del usuario e información del monedero con sólo acercar el dispositivo NFC en cualquier momento del programa, todo ello de forma segura.
3. Añadir un mecanismo de inserción y eliminación de productos de forma sencilla a través de una conexión con la base de datos SQLite por parte del personal de mantenimiento.
4. Implementar una interfaz de usuario más amigable y con posibilidad de hacer cambios de idioma

4.5.2 Sistema cliente

El sistema cliente está compuesto, en esencia, por dos elementos: el terminal móvil cliente y la tarjeta SIM que almacena el "applet" que da soporte al servicio de monedero electrónico.

4.5.2.1 Terminal cliente

El terminal cliente es el dispositivo móvil personal del usuario. Con él, el usuario será capaz de realizar transacciones contra un punto de venta con tan solo acercarlo al lector. Un terminal móvil puede ser cualquier tipo de dispositivo con la tecnología inalámbrica NFC pero normalmente el terminal cliente será un Smartphone.

Para que el terminal cliente funcione como dispositivo para realizar las compras es necesario que sea compatible tanto con la tecnología NFC, necesaria para proveer a la SIM de una antena para las comunicaciones, como con las Open Mobile APIs (*véase "Open Mobile APIs"*), necesarias para permitir a las aplicaciones del dispositivo móvil intercambiar comandos y respuestas APDU con la tarjeta SIM. Realmente estas APIs no serían necesarias para establecer una comunicación entre POS y SIM, pero si se quiere tener una aplicación móvil que consulte el saldo que queda o nos autentique para realizar las compras, es necesario disponer de ellas. Por ello, y tal y como se especifica en los requisitos de nuestro sistema, se ha implementado una aplicación que nos permita comunicarnos con el monedero electrónico de nuestra tarjeta SIM. La aplicación ha sido bautizada como NFCWallet y se describe en el siguiente apartado.

4.5.2.1.1 NFCWallet (Android)

Objetivos

El objetivo principal de esta aplicación es el de proporcionar los mecanismos necesarios para controlar, desde una aplicación en un teléfono móvil, el estado de nuestro monedero electrónico de la SIM.

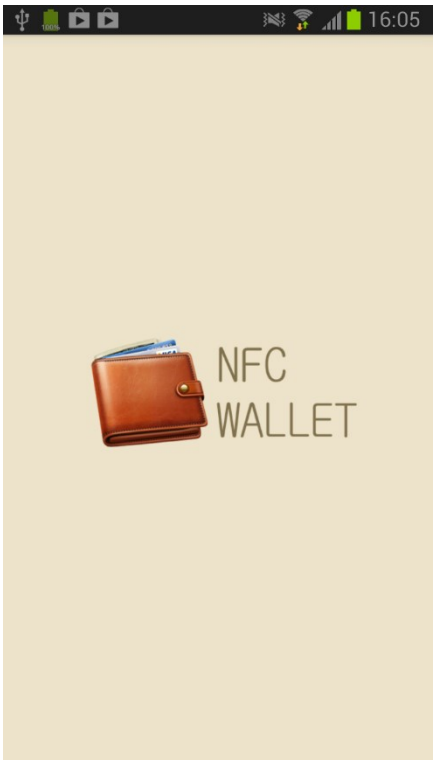

Figura 19: NFCWallet

Alcance

El alcance abarca la creación de una aplicación para el sistema operativo Android que permita consultar saldo, ingresar fondos, autenticarse y reclutar datos biométricos en el "applet" de monedero electrónico habilitado en nuestra tarjeta SIM.

Requisitos

- Capacidad para consultar el saldo del monedero electrónico
- Capacidad para ingresar fondos en el monedero, una vez el usuario ha sido autenticado
- Capacidad para realizar una autenticación biométrica con iris en el monedero electrónico
- Capacidad para reclutar datos biométricos del iris en el monedero electrónico
- La autenticación del usuario es por un tiempo limitado, transcurrido el cual, el sistema desautorizará al usuario.

- La captura de datos biométricos se hará, por simplicidad y por falta de la tecnología necesaria, mediante la selección de una imagen en la galería de fotografías del dispositivo móvil.

Funcionamiento

El funcionamiento de la aplicación NFCWallet es sencillo e intuitivo. En líneas generales, la aplicación consta de cuatro botones en la pantalla principal que proporcionan las cuatro funciones descritas en los requisitos: consultar saldo, ingresar fondos, autenticar y reclutar *(véase "Figura 20: Diagrama de flujo general NFCWallet (Android)"*).

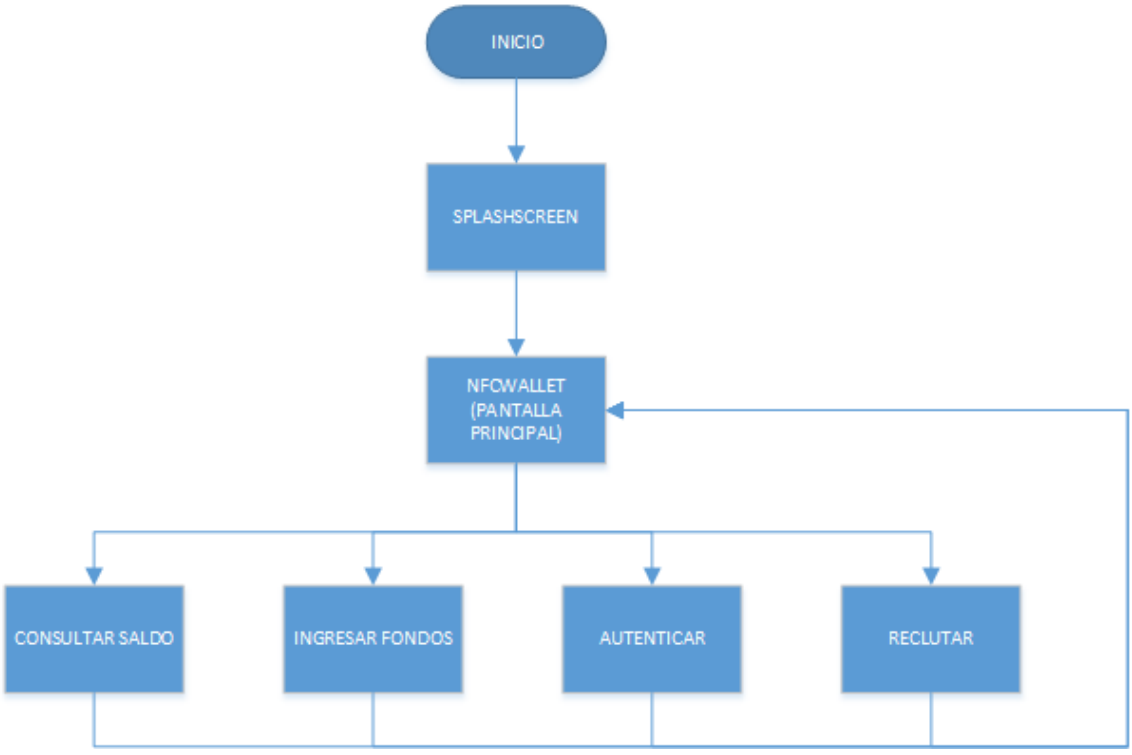

Figura 20: Diagrama de flujo general NFCWallet (Android)

La aplicación, tal como se mencionó anteriormente, está escrita en Android y la estructura de ficheros empleada es la siguiente:

- *NFCWallet.java:* Activity principal de la aplicación. En él están codificadas las funciones de consultar saldo e ingresar fondos. Proporciona el acceso a las activities de "Reconocimiento.java" y "Reclutamiento.java", donde se encuentran las otras dos funciones de la aplicación.
- *EnviarImagen.java:* Activity que contiene las pantallas tanto de reclutamiento como de reconocimiento, es decir, donde el usuario selecciona una imagen de la galería para enviar a la tarjeta SIM para su almacenamiento o comparación.
- *EventoSIM.java:* Activity empleada para capturar eventos recibidos de la tarjeta SIM. Se utiliza para detectar que el usuario ha intentado realizar una compra sin estar autenticado.
- *Utilidades.java:* Clase java que contiene funciones útiles tales como transformar un número decimal a un array de 3 bytes y viceversa. Se emplea para que las cantidades en decimal sean consistentes con la forma de tratar es tipo de números por la aplicación del monedero electrónico de la SIM (ver "*Manejo de las cantidades decimales*").
- *SplashScreenActivity.java:* Activity empleada para mostrar la pantalla de presentación de la aplicación.

Como se puede observar, los ficheros más importantes son los tres primeros ya que contienen todas les funciones requeridas, las cuales se describen a continuación en detalle.

Consultar Saldo

Función que obtiene el saldo disponible del monedero electrónico (*véase "Figura 21: Diagrama de flujo Consultar Saldo"*).

Figura 21: Diagrama de flujo Consultar Saldo

Como se puede ver en el diagrama de flujo, las operaciones a realizar son las siguientes:

1. Se envía el APDU habilitado en el applet del monedero de la SIM para consultar el saldo (*véase "Obtener Balance"*).
2. Se espera a recibir la respuesta con la cantidad deseada.
3. Si la respuesta ha sido de éxito, se extrae la cantidad contenida en el campo "data" del APDU de respuesta y se muestra al usuario en un mensaje. En caso de haberse producido algún error, se muestra al usuario un mensaje indicando que se vuelva a intentar la operación.

Ingresar Fondos

Función que ingresa una cierta cantidad de dinero introducida por el usuario a los fondos del monedero electrónico (*véase "Figura 22: Diagrama de flujo Ingresar Fondos"*).

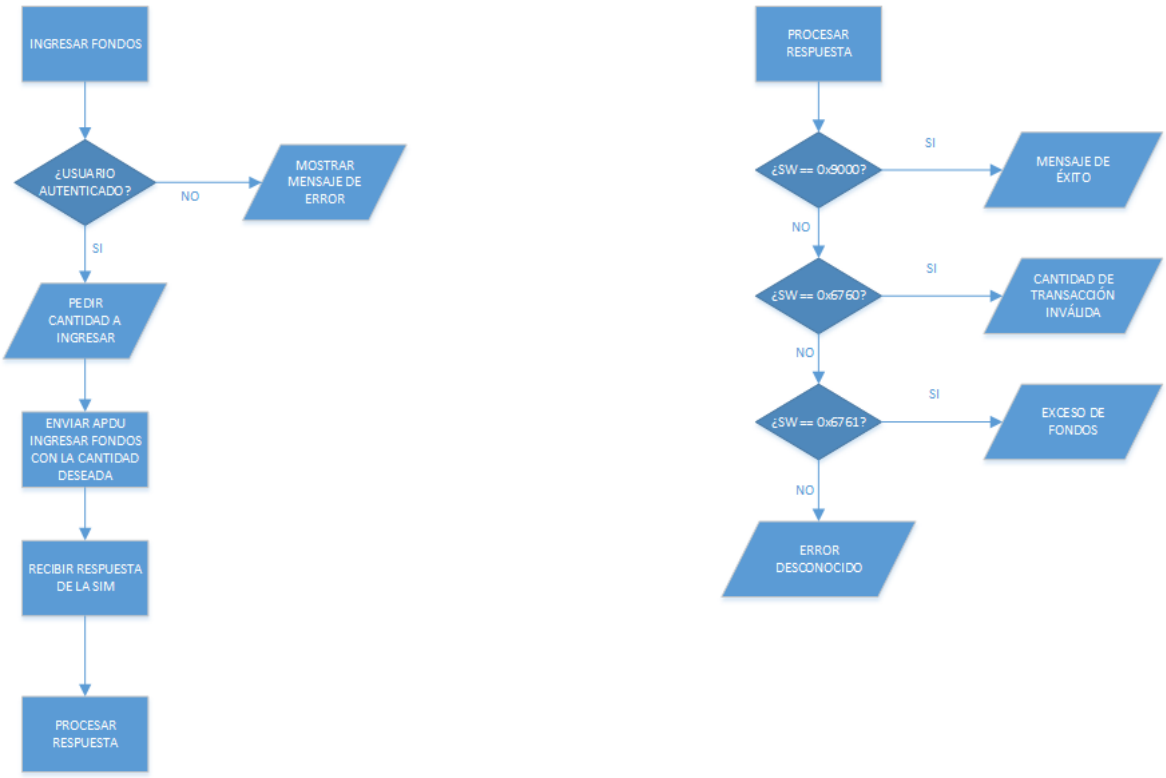

Figura 22: Diagrama de flujo Ingresar Fondos

A continuación se detallan las operaciones a realizar:

1. Se comprueba que el usuario esté autenticado. Esta comprobación se hace mediante un flag habilitado a tal efecto en la propia aplicación NFCWallet, y no mediante un comando APDU hacia la tarjeta SIM.
2. Si el usuario está autenticado se procede con el paso 3, mientras que si no lo está se muestra un mensaje de advertencia al usuario indicándole que debe autenticarse primero para proseguir con la operación.
3. Se pide al usuario la cantidad en euros que desea agregar a su monedero electrónico
4. Se envía a la tarjeta una el comando APDU de ingresar fondos junto con la cantidad introducida por el usuario (*véase "Ingresar Fondos"*).

5. Una vez haya sido recibida, se procesa la respuesta procedente de la tarjeta SIM con cuatro posibles casos descritos a continuación:
    a. La respuesta es 0x9000, en cuyo caso significa que la operación ha sido realizada con éxito.
    b. La respuesta es 0x6760 (*véase "Cantidad de Transacción Inválida"*).
    c. La respuesta es 0x6761 (*véase "Exceso de Fondos"*).
    d. La respuesta no es ninguna de las anteriores. Error desconocido.

Autenticación

Función que recibe los datos biométricos del usuario mediante la selección de una imagen de la galería y los envía a la tarjeta SIM para su comparación con los datos reclutados (*véase "Figura 23: Diagrama de flujo Autenticar"*).

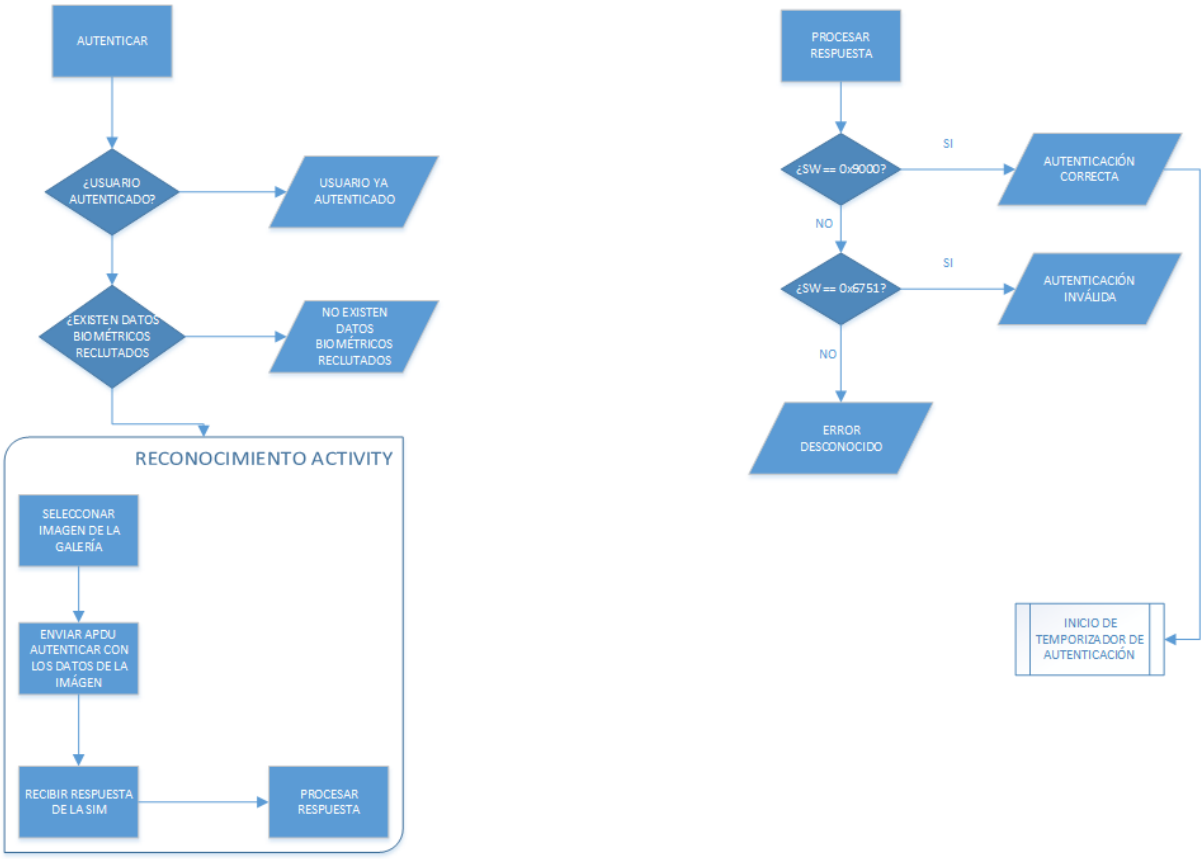

Figura 23: Diagrama de flujo Autenticar

La lógica de la función es la siguiente:

1. Se comprueba si el usuario ya está autenticado mediante un flag habilitad a tal efecto. En casi afirmativo se muestra un mensaje indicando que el usuario ya se encuentra autenticado, mientras que en caso contrario se pasa al siguiente paso.
2. Se comprueba si existen datos biométricos reclutados en la tarjeta mediante el envío de un comando habilitado para ello (*véase "Comprobar Datos Biométricos"*). Pueden darse dos casos:
    a. Sí hay datos biométricos reclutados. En este caso se procede con el paso 4.
    b. No existen datos biométricos en la tarjeta. En este caso se muestra un mensaje al usuario en que se le da la oportunidad de ir a la pantalla de reclutamiento.

3. Aparece la pantalla de reconocimiento donde el usuario selecciona una imagen de la galería con la que desea realizar la autenticación (*véase "Figura 24: Reconocimiento NFCWallet (Android)").*

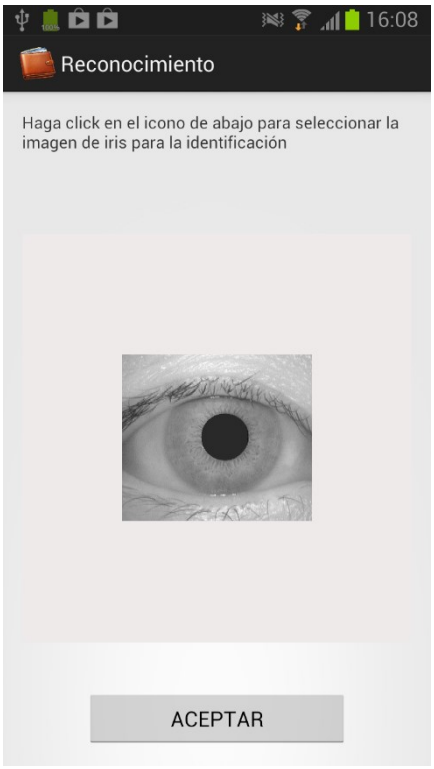

Figura 24: Reconocimiento NFCWallet (Android)

4. Se envía el comando de autenticación (*véase "Reconocer Datos Biométricos"*) junto con los datos de la imagen seleccionada. Los datos se envían en varios APDUs ya que normalmente una imagen no cabe en una sola trama.
5. Se espera a la respuesta de la tarjeta SIM. Pueden darse tres casos:
    a. Respuesta 0x9000. La imagen enviada coincide en un cierto porcentaje con la imagen reclutada. Usuario autenticado con éxito. En este momento se acciona un temporizador durante el cual el usuario se encuentra autenticado. Una vez que el temporizador venza, la aplicación mandará un APDU de finalización (*véase "Finalizar Autenticación"*) para finalizar con la autorización del usuario en el sistema.
    b. Respuesta 0X6751 (*véase "Datos Biométricos Inválidos"*).

c. La respuesta no es ninguna de las anteriores. Se ha producido un error desconocido.

Reclutamiento

Función que recibe los datos biométricos del usuario mediante la selección de una imagen de la galería y los envía a la tarjeta SIM para su almacenamiento (*véase "Figura 25: Diagrama de flujo Reclutar"*).

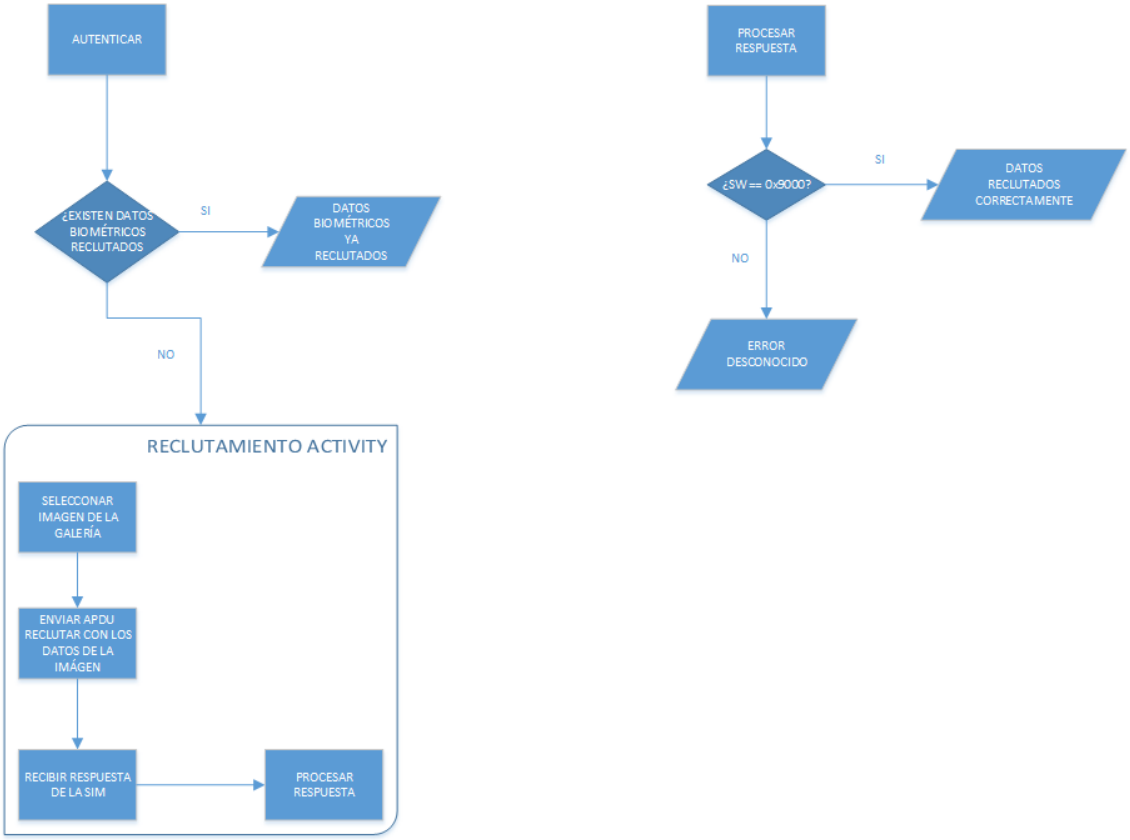

Figura 25: Diagrama de flujo Reclutar

A continuación de describe el detalle de la lógica de la función:

1. Se comprueba si existen datos biométricos reclutados en la tarjeta mediante el envío de un comando habilitado para ello (*véase "Comprobar Datos Biométricos"*). Pueden darse dos casos:

a. Sí hay datos biométricos reclutados. En este caso, y sólo si el usuario no se encuentra autenticado, se muestra un mensaje indicando que ya existen datos biométricos reclutados. En caso de que el usuario se encuentre autenticado se procede con el paso 2.
b. No existen datos biométricos en el monedero. Se procede con el paso 2.

2. Aparece la pantalla de reclutamiento donde el usuario selecciona una imagen de la galería con la que desea reclutarse.
3. Se envía el comando de reclutamiento (*véase "Reclutar Datos Biométricos"*) junto con los datos de la imagen seleccionada. Los datos se envían en varios APDUs ya que normalmente una imagen no cabe en una sola trama.
4. Se espera a la respuesta de la tarjeta SIM. Pueden darse dos casos:
   a. Respuesta de éxito 0x9000. El reclutamiento se ha realizado correctamente. A partir de este momento la información biométrica del usuario se encuentra almacenada en la tarjeta SIM.
   b. Otra respuesta. Se ha producido un error desconocido.

4.5.2.2 Tarjeta SIM NFC

La tarjeta SIM NFC quizás sea el elemento más complicado de nuestro sistema ya que conforma una compleja estructura de datos y protocolos de seguridad para establecer la comunicación con el exterior. Una tarjeta SIM NFC no es la tarjeta SIM normal y corriente que nos permite conectarnos a la red GSM, sino que es una tarjeta que, además de proporcionarnos la funcionalidad de una normal, nos permite realizar transacciones inalámbricas mediante NFC, es decir, nos proporciona la funcionalidad de "card emulation" descrita en el apartado 3.2.4.

Para conseguir esta funcionalidad, las tarjetas SIM NFC disponen de un protocolo de comunicación denominado SWP (*Single Wire Protocol*) que permite el intercambio de información entre el chip NFC de un móvil (CLF) y la propia tarjeta. Este protocolo, totalmente independiente del sistema operativo del teléfono móvil, permite por tanto,

acoplar de manera sencilla una antena a nuestra tarjeta SIM, permitiendo realizar transacciones incluso con el terminal móvil apagado.

En el ámbito de nuestro TFG vamos a implementar un "applet" JavaCard bautizado con el nombre de "NFCWallet" para una tarjeta SIM NFC que proporcione la funcionalidad de un monedero electrónico.

4.5.2.2.1 NFCWallet (JavaCard)

Objetivos

El objetivo principal de esta aplicación es proveer de un "applet" de pruebas de monedero electrónico al sistema de transacciones de este TFG.

Alcance

El alcance comprende la realización de un "applet" JavaCard que tenga las funciones básicas de un monedero electrónico. Dichas funciones se describen a continuación.

Requisitos

- Almacenar dinero del cliente
- Almacenar datos biométricos de iris del usuario
- Capacidad de realizar débitos
- Capacidad de realizar ingresos
- Capacidad de consultar saldo
- Capacidad de reclutar datos biométricos de iris
- Capacidad de autenticar al usuario mediante la comparación de datos biométricos en el interior de la tarjeta.
- Capacidad de enviar notificaciones a la aplicación del terminal cliente para avisar al usuario de cualquier interacción con el terminal.

Funcionamiento

El "applet" de monedero electrónico NFCWallet consiste en un conjunto de funciones JavaCard que proporcionan las características mencionadas en el apartado anterior. La aplicación NFCWallet se encuentra codificada en los dos ficheros descritos a continuación:

- *NFCWallet.java:* Es el "applet" como tal. Contiene todas las funciones que definen la estructura de un applet tales como "install", "select" o "process", además de las funciones propias de nuestra aplicación de monedero electrónico.
- *NumeroDecimal.java:* En esta clase se define la estructura y operaciones básica de un número decimal (*véase "Manejo de las cantidades decimales"*).

Como se puede ver, las funciones requeridas se encuentran en el primer fichero. Cada función se ejecuta al recibir un comando APDU concreto del exterior por lo que para ilustrar esta sección se ha hecho una recopilación de todos los posibles comandos APDU que se pueden recibir y la funcionalidad exigida por los requisitos que proporciona cada uno. Asimismo se enumeran y describen en detalle todas las posibles respuestas del "applet" a los comandos recibidos (*véase "Figura 26: Diagrama de flujo general NFCWallet (JavaCard)"*).

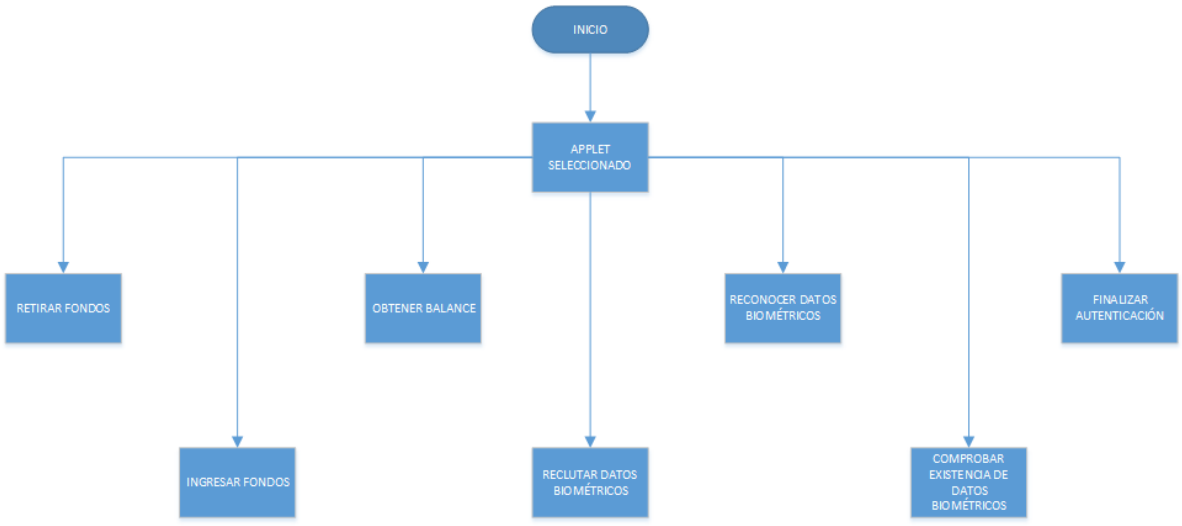

Figura 26: Diagrama de flujo general NFCWallet (JavaCard)

Comandos APDU

Retirar Fondos

El comando es el "*80 01 00 00 xx [cantidad a retirar en hexadecimal]*"

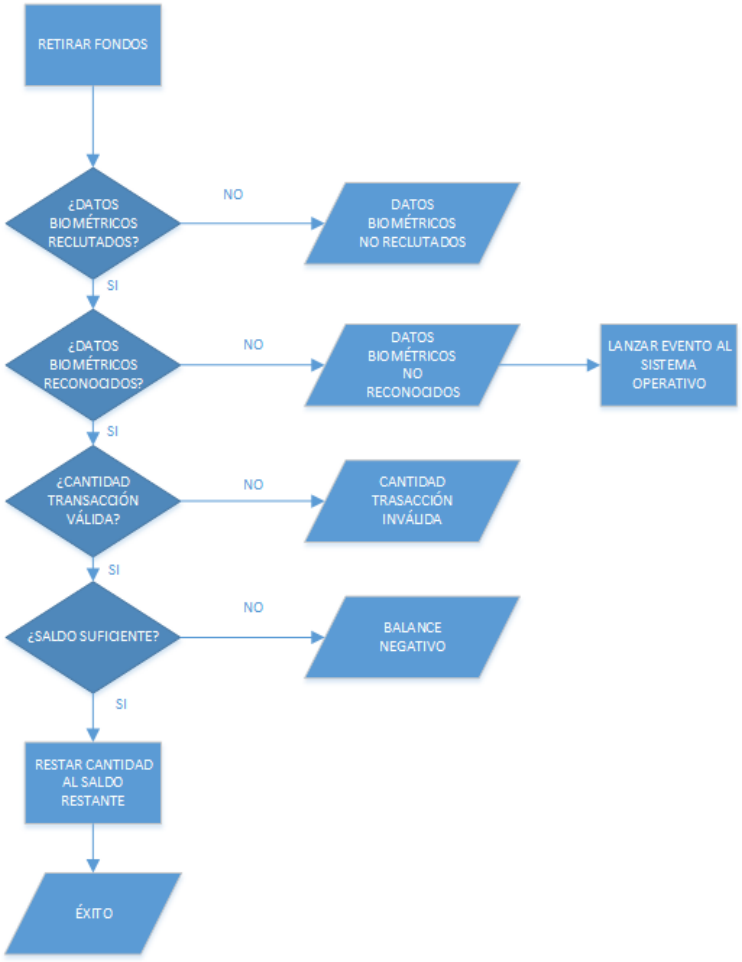

Figura 27: Diagrama de flujo Retirar Fondos

Esta función permite retirar dinero del monedero electrónico. Es la función enviada por el POS para descontar el importe referente a un producto. El modo de proceder al recibir el comando es el siguiente:

1. Se comprueba que haya datos reclutados en la tarjeta, y si no los hay se envía una respuesta de error "*DATOS BIOMÉTRICOS NO RECLUTADOS (0x6753)*".
2. Se comprueba que el usuario esté autenticado en la aplicación, y en caso de no ser así, se retorna una respuesta de error "*DATOS BIOMÉTRICOS NO VALIDADOS*

(0x6750)" y se envía un evento a la aplicación del terminal móvil indicando el error (empleando las APIs de SWP/HCI).

3. Se comprueba que la cantidad recibida no supere la permitida para una única transacción. En caso contrario se devuelve una respuesta de error "*CANTIDAD TRANSACCIÓN INVÁLIDA (0x6760)*".
4. Se comprueba que, tras hacer el débito, no quede un balance negativo en el saldo del monedero electrónico. En caso contrario se retorna una respuesta de error "*BALANCE NEGATIVO (0x6762)*".
5. Se realiza el cargo del importe en la cuenta a modo de transacción.
6. En caso de éxito se retorna una respuesta de éxito "(0x9000)" junto con la cantidad de dinero restante en el monedero electrónico.

Ingresar Fondos

El comando es el "*80 02 00 00 xx [cantidad a ingresar en hexadecimal]*"

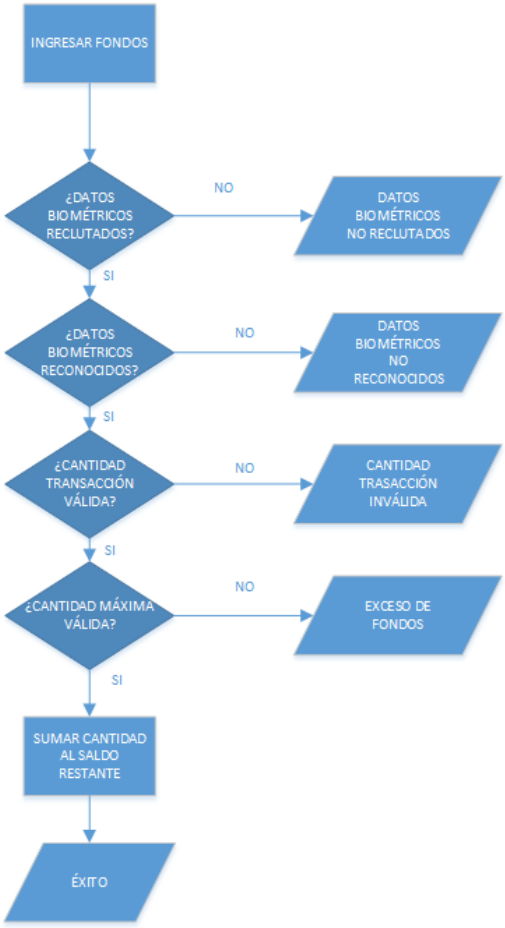

Figura 28: Diagrama de flujo Ingresar Fondos

Esta función permite ingresar dinero en el monedero electrónico. Es la función enviada por la aplicación del terminal cliente para realizar una recarga de saldo con el importe deseado. El modo de proceder al recibir el comando es el siguiente:

1. Se comprueba que haya datos reclutados en la tarjeta, y si no los hay se envía una respuesta de error "*DATOS BIOMÉTRICOS NO RECLUTADOS (0x6753)*".
2. Se comprueba que el usuario esté autenticado en la aplicación, y en caso de no ser así, se retorna una respuesta de error "*DATOS BIOMÉTRICOS NO VALIDADOS (0x6750)*".
3. Se comprueba que la cantidad recibida no supere la permitida para una única transacción. En caso contrario se devuelve una respuesta de error "*CANTIDAD TRANSACCIÓN INVÁLIDA (0x6760)*".

4. Se comprueba que, tras hacer el ingreso, no quede un balance superior al permitido por el monedero electrónico. En caso contrario se retorna una respuesta de error "*EXCESO DE FONDOS (0x6761)*".
5. Se realiza el ingreso del importe en la cuenta a modo de transacción.
6. En caso de éxito se retorna una respuesta de éxito "(0x9000)" junto con la cantidad de dinero restante en el monedero electrónico.

Obtener Balance

El comando es el "*80 03 00 00 00*"

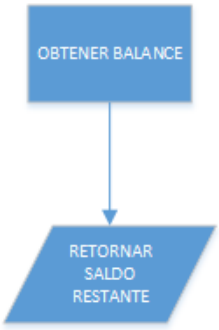

Figura 29: Diagrama de flujo Obtener Balance

Esta función permite obtener la cantidad de dinero almacenado en el monedero electrónico. El modo de proceder al recibir el comando es el siguiente:

1. Se retorna la cantidad de dinero del monedero sin hacer comprobación de ningún tipo. En caso de éxito se devuelve la respuesta de éxito *"(0x9000)"* junto con la cantidad de dinero restante.

Reclutar Datos Biométricos

En este caso tenemos dos tipos de comandos, diferenciados únicamente en el "CLA":

- *90 04 00 00 FF [primera y posteriores tramas de datos biométricos]*
- *80 04 00 00 xx [última trama de datos biométricos]*

La razón de emplear don tipos de comando es porque los datos biométricos son demasiado grandes como para enviarlos en un solo comando, por lo que en este caso se emplea el mecanismo de "chaining" proporcionado por el estándar para encadenar datos de diferentes APDUs.

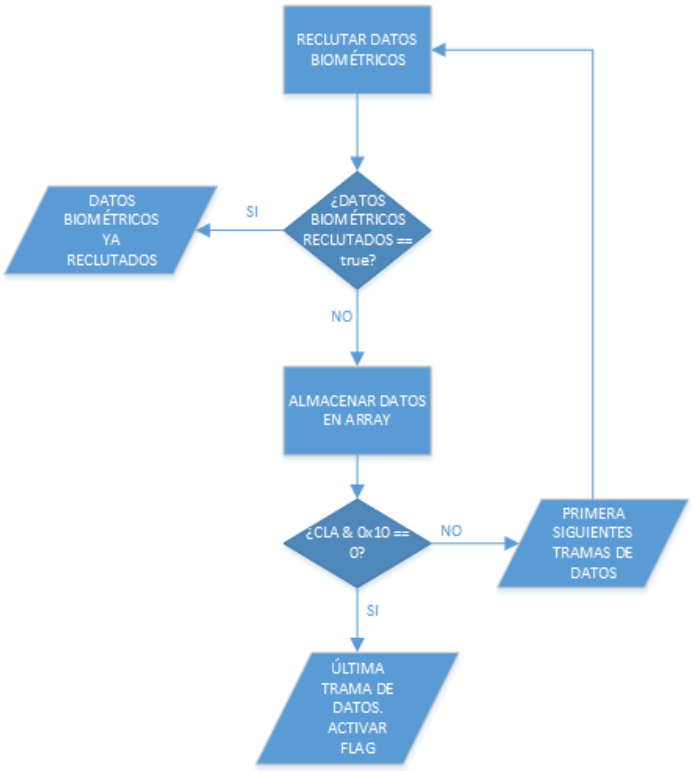

Figura 30: Diagrama de flujo Reclutar Datos Biométricos

Esta función enviar los datos biométricos del iris del usuario a las tarjeta SIM para su posterior comparación en las sucesivas autenticaciones. El modo de proceder al recibir el comando es el siguiente:

1. Se comprueba si hay datos biométricos reclutados en la tarjeta y si el usuario no está autenticado. Si esto sucede se retorna la respuesta de error "*DATOS BIOMÉTRICOS YA RECLUTADOS (0x6752)*". Esto se comprueba para evitar que un usuario no autenticado sea capaz de sobrescribir los datos biométricos del usuario legítimo.
2. Se van almacenando sucesivamente los datos biométricos del usuario en un array establecido a tal efecto hasta que se reciba el comando final (con CLA 0x80),

momento en el cual, si todo ha ido bien, se retorna un mensaje de éxito *"(0x9000)"*.

Reconocer Datos Biométricos

Nuevamente tenemos dos tipos de comandos, diferenciados únicamente en el "CLA":

- *90 05 00 00 FF [primera y posteriores tramas de datos biométricos]*
- *80 05 00 00 xx [última trama de datos biométricos]*

La razón de emplear don tipos de comando es exactamente la misma que en apartado anterior.

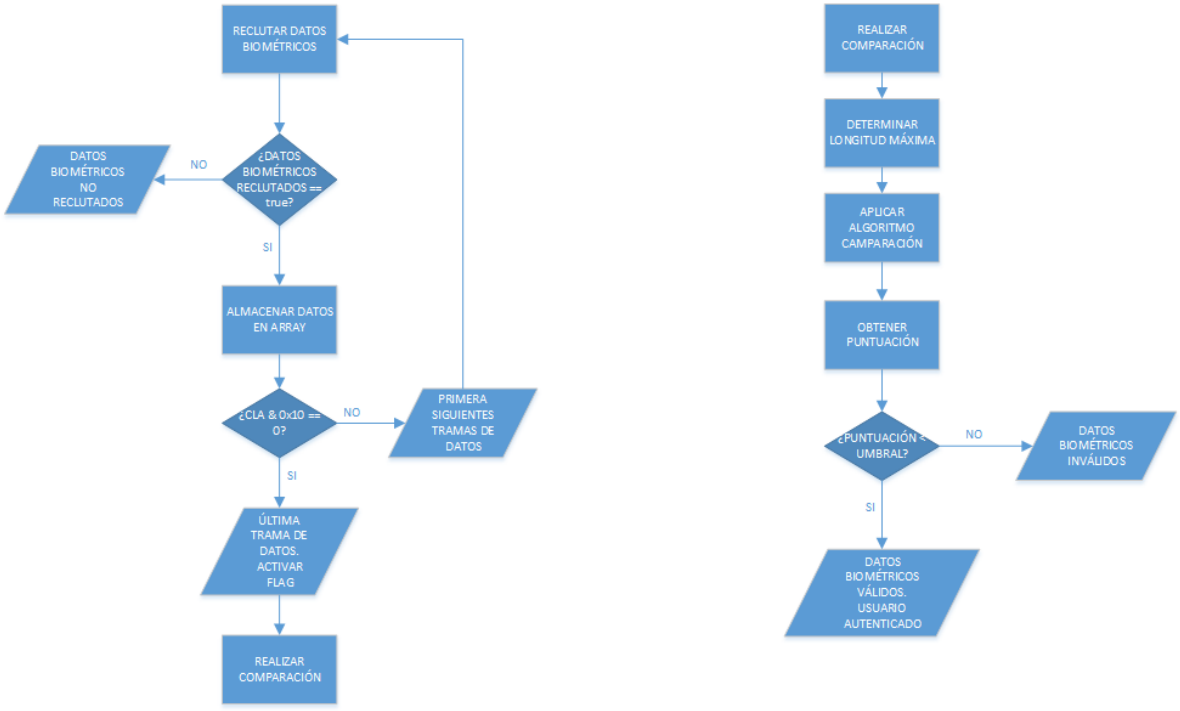

Figura 31: Diagrama de flujo Reconocer Datos Biométricos

Esta función envía los datos biométricos del iris del usuario a la tarjeta SIM para su comparación con los datos reclutados en la tarjeta anteriormente. El modo de proceder al recibir el comando es el siguiente:

1. Se comprueba si hay datos biométricos reclutados en la tarjeta y si el usuario no está autenticado. En caso contrario se retorna la respuesta de error "*DATOS*

BIOMÉTRICOS NO RECLUTADOS (0x6753)". Esto se comprueba para asegurarnos de que hay datos biométricos reclutados con los que comparar los que se van a recibir.

2. Se van almacenando sucesivamente los datos biométricos del usuario en un array establecido a tal efecto hasta que se reciba el comando final (con CLA 0x80).
3. Una vez recibidos los datos biométricos se procede a realizar su comparación con los almacenados en la tarjeta. Para ello se hace la función XOR sobre los dos arrays de datos y se cuenta el número de unos del array resultante. De esta manera podemos tener una idea de las diferencias entre las dos tramas de datos biométricos.
4. Se compara el número de unos hallado con un umbral calculado en base a la longitud de los datos biométricos. Si el número de unos supera el umbral se retorna una respuesta de error "*DATOS BIOMÉTRICOS INVÁLIDOS (0x6751)*", mientras que si no lo supera o es igual, quiere decir que la comparación ha sido exitosa y por tanto se retorna una respuesta de éxito *"(0x9000)".*

Comprobar Datos Biométricos

El comando es el *"80 06 00 00 00"*.

Figura 32: Diagrama de flujo Comprobar Datos Biométricos

Este comando adicional sirve para comprobar si existen datos biométricos reclutados en la tarjeta. El modo de proceder es el siguiente:

1. Se comprueba si existen datos biométricos reclutados. En caso negativo se retorna la respuesta de error "*DATOS BIOMÉTRICOS NO RECLUTADOS (0x6753)*".
2. En caso de éxito se retorna una respuesta de éxito *"(0x9000)".*

Finalizar Autenticación

El comando es el *"80 07 00 00 00"*.

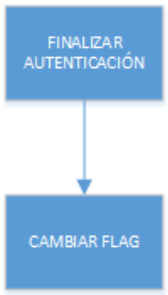

Figura 33: Diagrama de flujo Finalizar Autenticación

Este comando adicional sirve para finalizar el acceso a las funciones que requieren autenticación por parte del usuario. Este comando se utiliza en la aplicación del terminal cliente cuando finaliza el tiempo en que el usuario está autenticado, sirve para desautorizar al usuario en la tarjeta. El modo de proceder es el siguiente:

1. Se cambia el estado del flag que define si el usuario está o no autenticado y se devuelve una respuesta de éxito *"(0x9000)".*

Respuestas APDU

Datos Biométricos No Validados

Código de respuesta: *0x6750*

Esta respuesta indica que no se han validado los datos biométricos, es decir, el usuario no ha sido autenticado.

Datos Biométricos Inválidos
Código de respuesta: *0x6751*

Esta respuesta indica que los datos biométricos introducidos no se corresponden con los reclutados.

Datos Biométricos Ya Reclutados
Código de respuesta: *0x6752*

Esta respuesta indica que ya existen datos biométricos reclutados en la tarjeta.

Datos Biométricos No Reclutados
Código de respuesta: *0x6753*

Esta respuesta indica que no existen datos biométricos reclutados en la tarjeta.

Cantidad de Transacción Inválida
Código de respuesta: *0x6760*

Esta respuesta indica que se ha superado la cantidad límite para una única transacción en el monedero electrónico.

Exceso de Fondos
Código de respuesta: *0x6761*

Esta respuesta indica que se ha superado el límite de fondos admitido por el monedero electrónico.

Balance Negativo
Código de respuesta: *0x6762*

Esta respuesta indica que no existen fondos suficientes para realizar la transacción deseada.

Manejo de las cantidades decimales

Dada la imposibilidad de manejar cantidades numéricas con decimales en el sistema operativo JavaCard, se ha ideado un mecanismo para poder manejar, enviar y recibir dichas cantidades sin que afecte al funcionamiento del sistema. Este mecanismo consiste en la definición de un número de 3 bytes, donde los dos primeros conforman la parte entera y el último constituye la parte decimal.

```
public NumeroDecimal(short parteEntera, byte parteDecimal){
        this.parteEntera = parteEntera;
        this.parteDecimal = parteDecimal;
}
```

Este mecanismo sencillo simplemente divide en dos el número y trata cada una de las partes como si fuera un número entero. Asimismo se han definido una serie de operaciones matemáticas básicas necesarias para el funcionamiento de la aplicación, tales como la suma, resta o comparación entre números.

```
public static NumeroDecimal suma(NumeroDecimal a, NumeroDecimal b){
        NumeroDecimal resultado = new NumeroDecimal();
        short sumaPrevia;
        sumaPrevia = (short)((short)a.getParteDecimal()+(short)b.getParteDecimal());
        if(sumaPrevia >= (short)DECIMAL_MAXIMO){
                resultado.setParteDecimal((byte)(sumaPrevia-DECIMAL_MAXIMO));
                b.setParteEntera((short)(b.getParteEntera()+(short)1));
        }
        else{
                resultado.setParteDecimal((byte)sumaPrevia);
        }

        resultado.setParteEntera((short)(a.getParteEntera()+b.getParteEntera()));
        return resultado;
}
```

```
public static NumeroDecimal resta(NumeroDecimal a, NumeroDecimal b){
        NumeroDecimal resultado = new NumeroDecimal();
        if(a.getParteDecimal()<b.getParteDecimal()){
                resultado.setParteDecimal((byte)((a.getParteDecimal()+DECIMAL_MAXIMO)-
                                b.getParteDecimal()));
                b.setParteEntera((short)(b.getParteEntera()+(short)1));
                resultado.setParteEntera((short)(a.getParteEntera()-
                        b.getParteEntera()));
        }
        else{
                resultado.setParteDecimal((byte)(a.getParteDecimal()-
                        b.getParteDecimal()));
                resultado.setParteEntera((short)(a.getParteEntera()-
                        b.getParteEntera()));
        }
        return resultado;
}
```

```
public static boolean menorQue(NumeroDecimal a, NumeroDecimal b){

if(((a.getParteEntera()==b.getParteEntera())&&(a.getParteDecimal()<b.getParteDecimal()))
        ||a.getParteEntera()<b.getParteEntera())
        return true;
return false;
}
```

4.6 Pruebas realizadas

Para el correcto funcionamiento del software implementado se han realizado una serie de pruebas con unos dispositivos descritos a continuación:

- *Google Nexus 7:* Empleado como POS para probar el sistema de simulación de máquina expendedora de bebidas.
- *Samsung Galaxy Note II:* Empleado como terminal cliente en el sistema de transacciones. Este dispositivo cuenta con NFC y es compatible con las Open Mobile APIs de SimAlliance (*véase "Open Mobile APIs"*).
- *Tarjeta SIM NFC Gemalto UpTeq2.0:* Empleada como tarjeta SIM NFC para la implementación del applet de monedero electrónico. Esta tarjeta dispone de la última versión de JavaCard y es compatible con el Amendment C de GlobalPlatform, el cual especifica la gestión de aplicaciones sin contactos en una tarjeta JavaCard.

Para la realización de las pruebas se han tenido en cuenta los puntos críticos donde el sistema es más vulnerable a fallos. El esquema de desarrollo empleado ha sido de desarrollo ágil, el cual ha permitido conseguir solucionar errores mediante pruebas periódicas y frecuentes del software de manera rápida.

Las pruebas realizadas se describen en detalle en los siguientes apartados, en los cuales se mostrarán algunas capturas de pantalla para ilustrar, de manera gráfica, el entorno desarrollado.

4.6.1 Compra de un producto del POS con usuario no autenticado

Para la ejecución de esta prueba se han llevado a cabo los siguientes pasos:

- Seleccionamos un producto en la aplicación Soft-drink Shop del punto de venta, en nuestro caso el terminal Nexus 7.
- Cuando nos lo pida la aplicación, acercamos el terminal móvil cliente al POS para efectuar el pago

El resultado de la prueba ha sido el siguiente:

- La aplicación del POS lanza un mensaje indicando que el usuario no se encuentra autenticado en el sistema de monedero electrónico.
- La aplicación NFCWallet del terminal cliente lanza un mensaje indicando que el usuario no se encuentra autenticado e indicándole si desea ir a la aplicación para realizar la autenticación.

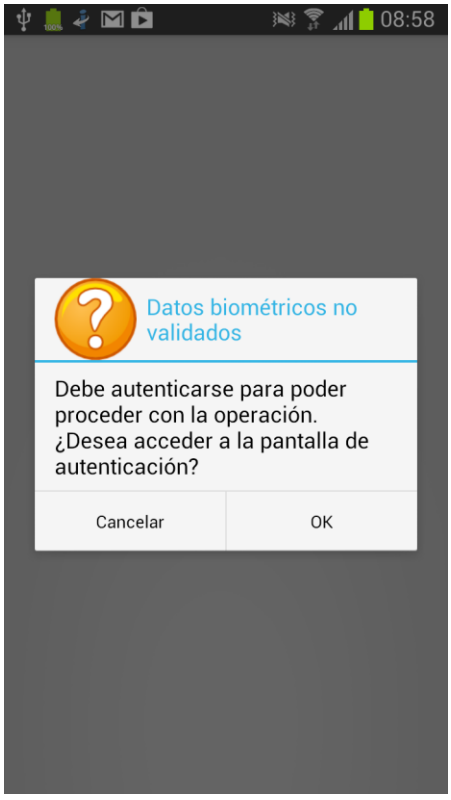

Figura 34: Evento NFCWallet

Tal y como se especificó en los requisitos, se ha comprobado que el comportamiento del sistema frente a esta prueba ha sido el esperado.

4.6.2 Compra de un producto del POS con usuario autenticado

Para la ejecución de esta prueba hemos llevado a cabo los siguientes pasos:

- Comprobamos mediante la aplicación NFCWallet del terminal Samsung Galaxy Note II el saldo del que disponemos en el monedero electrónico.
- Seleccionamos un producto en la aplicación Soft-drink Shop del punto de venta, en nuestro caso el terminal Nexus 7.
- Cuando nos lo pida la aplicación, acercamos el terminal móvil cliente al POS para efectuar el pago.
- Comprobamos el saldo restante y vemos si ha descendido nuestro saldo antes de realizar la compra.

El resultado de la prueba ha sido el siguiente:

- Al comprobar el saldo inicialmente mediante la aplicación NFCWallet se ha visto que la cantidad de dinero disponible era de 660.6€

Figura 35: Consultar saldo antes de la compra

- Se ha seleccionado un producto de 1.20€ en el POS. Al acercar el terminal cliente al punto de venta ha aparecido un mensaje en el punto de venta indicando que la compra se ha realizado con éxito, así como el saldo restante en el monedero, sea 659.4€.
- Al comprobar el saldo restante mediante la aplicación NFCWallet se ha comprobado que, efectivamente, el saldo ha descendido a 659.4€

Figura 36: Consultar saldo después de la compra

Así pues, se puede comprobar que el sistema responde satisfactoriamente ante las pruebas realizadas.

4.6.3 Autenticación de un usuario autenticado

Esta prueba presenta uno de los puntos críticos en la ejecución de la función de autenticar en el sistema. Se han llevado a cabo una los siguientes pasos para su ejecución:

- Entrar en la aplicación NFCWallet y autenticar satisfactoriamente a un usuario en el sistema
- Una vez autenticado, y dentro del tiempo en que la autenticación sigue vigente, intentar autenticar otra vez al usuario en el sistema

El comportamiento observado ha sido el siguiente:

- El periodo de vigencia de la autenticación vencía después del tiempo determinado contando a partir del momento en que se hizo la primera autenticación

Dado este resultado, comprueba que el resultado esperado debería ser que la autenticación finalizara pasado el tiempo determinado contando a partir de la última autenticación realizada.

El motivo de este comportamiento es a causa de que, cada vez que se realiza una autenticación se crea un subproceso a parte que inicia el temporizador que cuenta el tiempo restante de vigencia de la autenticación. De esta manera, cada vez que el usuario se autenticaba se creaba un nuevo subproceso totalmente independiente de los demás, por lo que a la finalización del primer subproceso lanzado, la aplicación realizaba la tarea de desautorización.

Solución: Se ha impuesto la restricción de que un usuario autenticado en el sistema no puede volver a autenticarse.

5. CONCLUSIÓN

Se pueden obtener varias conclusiones del trabajo desarrollado en este Trabajo Fin de Grado. La conclusión principal es acerca de las grandes posibilidades que nos ofrecen los smartphones a diferentes escenarios, especialmente cuando los combinamos con otras tecnologías tales como biometría o NFC. Los smartphones constituyen un importante centro de aplicaciones donde podemos realizar cualquier operación administrativa o bancaria en unos pocos minutos y de una manera rápida y sencilla. Adicionalmente, tal y como se muestra en el sistema desarrollado, la inclusión de otras tecnologías como NFC y biometría proporcionan una manera aún más cómoda de realizar nuestras operaciones, y lo que es más importante, una manera más segura de identificar a los usuarios cuando, por ejemplo, acceden a una aplicación bancaria. Por otro lado, NFC proporciona una forma de comunicación entre dispositivos a distancia permitiendo mayor rapidez y facilidad de uso para los usuarios, especialmente discapacitados. NFC permite realizar transferencias de datos entre smartphones, y entre smartphones y tarjetas inalámbricas, lo que añade un extra de seguridad en las operaciones.

Las tarjetas inteligentes y el sistema operativo JavaCard proporcionan una plataforma segura multi-aplicación donde el usuario puede disfrutar de numerosos servicios relacionados con operaciones bancarias, transporte público, etc. Además si empleamos esta tecnología dentro de las tarjetas SIM, nuestro teléfono móvil se convierte en un centro de datos personal y totalmente interactivo con todos estos servicios en la palma de nuestra mano.

Finalmente, la biometría nos proporciona lo que tan demandado se encuentra actualmente en cualquier sistema informático: la seguridad. Con estos mecanismos biométricos de autenticación podemos sentirnos protegidos y podemos estar seguros de la integridad y privacidad de nuestros datos.

El producto de todas estas tecnologías anteriores combinadas en una sola ha dado como resultado el producto desarrollado en este trabajo de fin de grado. Se ha conseguido desarrollar un sistema seguro, manejable y, sobretodo, innovador.

Definitivamente nos estamos acercando a una nueva era en sistemas de pagos bancarios e información en general donde los teléfonos móviles están ganando fuerza cada vez con mayor rapidez.

6. CONCLUSION

Several conclusions can be obtained from the work developed in this Bachelor Thesis. The main conclusion we obtained is the increasing number of possibilities a smartphone provides to different scenarios, especially when combined when other technologies as NFC or Biometrics. The smartphone has shown to be an important application centre where any administrative and banking operations can be performed in few minutes and in a comfortable manner. Additionally, as our implemented system has pointed out, the inclusion of other technologies such as biometrics and NFC provides an even more comfortable and what is more important, a secure way to identify users when for example, accessing to bank applications. NFC technology provides a contactless way to communicate devices and, therefore, it is faster and usable for all the users. In fact, this solution fits perfectly to disabled people with motor disabilities. NFC allows data transfers not only between smartphones, but also between them and smartcards. This provides not only comfort but also security.

Smartcards and JavaCard operating system provide a safe multi-application platform where the user can have many services related to banking, public transport, etc. Moreover if we use these smartcards as a SIM card, our smartphone will become our personal and interactive data centre with all of these services in the palm of our hand.

Finally biometrics provides us an important thing, increasingly demanded in our society: security. With the biometric mechanisms of authentication we can feel protected. We can be sure of the integrity and privacy of our banking data stored in our SIM and protected by sophisticated biometric algorithms.

All these facts have been combined into one system in the work developed in this Bachelor Thesis. The resulting system is a secure, comfortable and moreover, an

innovative system where an effective combination of NFC, smartcards, mobile devices and biometrics has been done in order to reach all those features in the same system.

Definitely we are approaching to a new era of banking and information in general where mobile devices are gaining strength and we will be able to perform most of our applications on them, avoiding us to go to banks, and providing us a safe way to perform them.

7. BIBLIOGRAFÍA

[1] R. Sánchez-Reillo, J. C. Acedo Jiménez, D. Cerezo Quesada and X. R. Rodríguez Lorenzo, La tecnología de las tarjetas inteligentes.

[2] C. E. Ortiz, "Oracle," 29 Mayo 2003. [Online]. Available: http://www.oracle.com/technetwork/java/javacard/javacard1-139251.html. [Accessed 9 Mayo 2013].

[3] V. Poulbere, "Gemalto," Septiembre 2007. [Online]. Available: http://www.gemalto.com/nfc/global_platform.html. [Accessed 9 Mayo 2013].

[4] G. Milette and A. Stroud, Professional Android Sensor Programming, Indianápolis: Wrox, 2012.

[5] ECMA-352, "ECMA," Junio 2010. [Online]. Available: http://www.ecma-international.org/publications/standards/Ecma-352.htm. [Accessed 9 Mayo 2013].

[6] "Nokia Developers," 27 Noviembre 2012. [Online]. Available: http://www.developer.nokia.com/Community/Wiki/Inside_NFC:_Usages_and_Working_Principles. [Accessed 9 Mayo 2013].

[7] "Nokia Developers," 27 Noviembre 2012. [Online]. Available: http://www.developer.nokia.com/Community/Wiki/Understanding_NFC_Data_Exchange_Format_(NDEF)_messages. [Accessed 9 Mayo 2013].

[8] "4 Android Fans," 10 Junio 2013. [Online]. Available: 4androidfans.wordpress.com.

[9] "Android," 1 Mayo 2013. [Online]. Available: http://developer.android.com/about/dashboards/index.html. [Accessed 9 Mayo 2013].

[10] "Hothardware," 16 Marzo 2011. [Online]. Available: http://hothardware.com/News/Google-Purportedly-Testing-NFC-Payment-Machines-In-NYSF-Stores-/. [Accessed 9 Mayo 2013].

8. ANEXO I: Planificación del trabajo

En este apartado se va a proceder a hacer un desglose de las tareas que se han llevado a cabo durante todo el transcurso del Trabajo de Fin de Grado así como el coste total incurrido en el proyecto desarrollado.

El desglose se ha dividido en varias fases para mayor comodidad del lector.

1. FASE 1: Documentación previa
    a. Estudio de la plataforma Android y su entorno de desarrollo (40 horas)
    b. Estudio de la plataforma JavaCard y su entorno de desarrollo (50 horas)
    c. Estudio de la tecnología de radiofrecuencia NFC (30 horas)
    d. Estudio de las características más importantes de las tarjetas inteligentes así como de algunos estándares como GlobalPlatform y ISO/IEC 14443 (30 horas)
    e. Estudio de las características generales de protocolo SWP así como de su utilización en tarjetas SIM NFC (20 horas)
2. FASE 2: Diseño y desarrollo del sistema
    a. Diseño de esquemas generales para el desarrollo del sistema así como protocolos necesarios de intercomunicación entre los distintos dispositivos (15 horas)
    b. Diseño e implementación de la aplicación Soft-drink Shop para el punto de venta (10 horas)
    c. Diseño e implementación del “applet” de monedero electrónico JavaCard para la tarjeta SIM del cliente (50 horas)
    d. Diseño e implementación de la aplicación NFCWallet del terminal cliente (50 horas)
3. FASE 3: Pruebas

a. Pruebas de la aplicación Soft-drink Shop en un terminal Google Nexus 7 (10 horas)
b. Pruebas de la aplicación NFCWallet en Samsung Galaxy Note II y pruebas junto con el "applet de monedero electrónico" para una correcta comunicación entre teléfono móvil y SIM (10 horas)
c. Pruebas de comunicación inalámbrica NFC entre móvil cliente y POS (10 horas)

4. FASE 4: Elaboración de la memoria
   a. Estructuración y elaboración de la memoria (50 horas)
   b. Corrección y maquetación (10 horas)

Tabla 3: Desglose de tareas

FASES	HORAS EMPLEADAS
Documentación previa	170
Diseño y desarrollo del sistema	125
Pruebas	30
Elaboración de la memoria	60
TOTAL	385

9. ANEXO II: Presupuesto

A continuación se dispone a realizar un pequeño presupuesto para poder contabilizar los costes totales del proyecto desarrollado, tanto de material como de personal. A continuación se muestra un desglose de las actividades realizadas así como de su tiempo y costo.

COSTES MATERIALES

Los materiales necesarios han sido un ordenador para realizar el desarrollo de las aplicaciones, dos teléfonos móviles para probar las aplicaciones del POS y del terminal cliente, una tarjeta SIM NFC para probar el funcionamiento del monedero electrónico y un lector de tarjetas para poder instalar contenidos en la SIM.

Así pues, considerando un periodo de amortización de 3 años y el tiemdo en cuenta el tiempo del proyecto, la relación de costes materiales quedarían como se expone a continuación:

Tabla 4: Costes materiales

CONCEPTO	PRECIO (€)
Ordenador de altas prestaciones	157
Samsung Galaxy Note II	73,44
Google Nexus 7 8Gb	33,83
Lector tarjetas dual SCM SCL010	13,60
TOTAL	**277,87**

COSTES DE PERSONAL

Para la realización de este proyecto ha sido necesario el trabajo de un jefe de proyecto y de un ingeniero.

Tabla 5: Costes de personal

OCUPACIÓN	HORAS	PRECIO/HORA	IMPORTE (€)
Jefe de proyecto	15	90	1350
Ingeniero	370	60	22200
TOTAL	385		23550

COSTES TOTALES

Tabla 6: Costes totales

CONCEPTO	PRECIO (€)
Costes materiales	277,87
Costes de personal	23550
Costes indirectos (20%)	4765,57
Subtotal	28593,44
IVA (21%)	6004,62
TOTAL	34598

El coste total del proyecto es de TREINTA Y CUATRO MIL QUINIENTOS NOVENTA Y OCHO euros

Leganés, 10 de Junio de 2012

El ingeniero